NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ANALYSIS, DESIGN AND IMPLEMENTATION OF A NETWORKING PROOF-OF-CONCEPT PROTOTYPE TO SUPPORT MARITIME VISIT, BOARD, SEARCH AND SEIZURE TEAMS

by

Van E. Stewart

March 2014

Thesis Co-Advisors:	Alex Bordetsky Albert Barreto

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY ***(Leave blank)***

2. REPORT DATE
March 2014

3. REPORT TYPE AND DATES COVERED
Master's Thesis

4. TITLE AND SUBTITLE
ANALYSIS, DESIGN AND IMPLEMENTATION OF A NETWORKING PROOF-OF-CONCEPT PROTOTYPE TO SUPPORT MARITIME VISIT, BOARD, SEARCH AND SEIZURE TEAMS

5. FUNDING NUMBERS

6. AUTHOR Van E. Stewart

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The United States Coast Guard (USCG) is composed of 42,000 men and women, spread over nine districts and 35 different sectors, who are tasked with the security and stewardship of our nations waters. The Coast Guard operates 244 cutters, 1776 small boats and 198 aircraft to meet the needs of its mission. The men and women operating these platforms are tasked with a variety of different mission sets that include maritime security operations, law enforcement, prevention, response, defense operations and marine transportation system management. In 2012, the USCG conducted over 1,700 security boarding's on high interest vessels that were bound for the United States. One of the most crucial factors for success during these high-risk evolutions is communications between the host USCG cutter and the men and women who comprise the boarding team.

14. SUBJECT TERMS MIO, VBSS, software defined radios

15. NUMBER OF PAGES
71

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

THIS PAGE INTENTIONALLY LEFT BLANK

ANALYSIS, DESIGN AND IMPLEMENTATION OF A NETWORKING PROOF-OF-CONCEPT PROTOTYPE TO SUPPORT MARITIME VISIT, BOARD, SEARCH AND SEIZURE TEAMS

Van E. Stewart
Lieutenant, United States Navy
B.S., University of Mississippi, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
March 2014

Author: Van E. Stewart

Approved by: Alex Bordetsky
Thesis Co-Advisor

Albert Barreto
Thesis Co-Advisor

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Coast Guard (USCG) is composed of 42,000 men and women, spread over nine districts and 35 different sectors, who are tasked with the security and stewardship of our nations waters. The Coast Guard operates 244 cutters, 1776 small boats and 198 aircraft to meet the needs of its mission. The men and women operating these platforms are tasked with a variety of different mission sets that include maritime security operations, law enforcement, prevention, response, defense operations and marine transportation system management. In 2012, the USCG conducted over 1,700 security boarding's on high interest vessels that were bound for the United States. One of the most crucial factors for success during these high-risk evolutions is communications between the host USCG cutter and the men and women who comprise the boarding team.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BER	bit error rate
BT	boarding team
C2	command and control
COTM	communications on the move
FYI	for your information
GGB	Golden Gate Bridge
IETF	Internet Engineering Task Force
LOS	line-of-site
MANETS	mobile ad-hoc networks
MIB	management information base
MIO	maritime interdiction operations
MPU	man portable unit
NLOS	non-line-of-site
NMS	network management system
NOC	Network Operation Center
OID	object identifier
QOS	quality of service
RF	radio frequency
RFC	request for comment
RHIB	rigid-hull-inflatable boat
RMON	remote network monitoring
SDR	software defined radios
SFPB	San Francisco police boat
STD	standard
TW	Trellisware
USCG	U.S. Coast Guard
VBSS	visit, board, search and seizure
VOI	vessel of interest
WMN	wireless mesh network
WR	WaveRelay

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to express my thanks to Dr. Alex Bordetsky and Buddy Barreto for giving me the opportunity, guidance, and patience to successfully complete my thesis. It has been an honor working with them, and I hope that their future research stays fruitful.

This would not be possible without the love and support of my wife, Christine. Every step of the way was filled with encouragement and faith because of her. I can’t wait to see our future son.

Thank you to my children, Marlee, Lexi, and Kendyll, for never letting me feel discouraged regardless of how far apart we were. Getting back to my three stooges was vital in reaching this goal.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The problem is that the United States military does not currently possess a communications platform that adequately provides continuous, reliable, and secure voice and data communications between the host naval vessel and the boarding team members that are deployed on large freighter vessels conducting operations.

B. PURPOSE STATEMENT

The purpose of this thesis is to construct a communication platform in a simulated maritime environment that provides continuous, reliable, and secure voice and data communications for a host naval vessel and boarding team members.

C. BENEFITS OF RESEARCH

The benefits of this thesis are to identify the strengths and weakness of mobile communication devices, and to identify network management capability gaps.

D. RESEARCH QUESTIONS

1. Does current software defined radio technology provide sufficient communication capabilities for U.S. Coast Guard maritime interdiction operations?
2. Does current network management systems allow the U.S. Coast Guard to manage wireless networks effectively?

E. THESIS STRUCTURE

1. Chapter I: Introduction

This chapter introduces and identifies the focus and purpose of the research conducted in order to address the current communication problems for maritime interdiction operations (MIO) conducted by visit, board, search and seizure (VBSS) teams.

2. Chapter II: Literature Review

This chapter provides the basic fundamental concepts that will explain the topics involved with the experiment.

3. Chapter III: Experiment

This chapter will discuss the details of the experiment conducted for VBSS communications in two separately simulated MIO environments, and the communication systems utilized to conduct both.

4. Chapter IV: Analysis

This chapter will provide the data collected, and conduct a comparative analysis of the two communication devices tested. The information will be evaluated for performance, and the results documented.

5. Chapter V: Conclusion

This chapter will summarize the analysis findings, and provide recommendations for possible future research.

II. LITERATURE REVIEW

A. VISIT, BOARD, SEARCH AND SEIZURE

1. Overview

According to Barker (2009) the term visit, board, search, and seizure (VBSS) describes the maritime boarding operations developed by the U.S. military and law enforcement agencies in order to thwart piracy, smuggling, and in some cases terrorism. Other missions include custom and safety inspections requiring the capabilities of today's navies, marines, and maritime police agencies. VBSS teams have become a vital asset in the Navy's twenty-first century maritime strategy whether it is searching a dhow in the Persian Gulf for contraband, or boarding a vessel suspected of piracy near the Horn of Africa (Barker, 2009). Nguyen and Baker (2012) states that in order to enforce embargoes, intercept contrabands, prevent drug and human smuggling, and fight piracy, the U.S. Navy conducts thousands of maritime interdiction operations a year. Typically conducted by eight-man VBSS teams using rigid-hull-inflatable boats (RHIB) or helicopters, these operations often take place miles from the base ship in hostile environments. Many of the VBSS operations are conducted on compliant vessels, that is, the target ship cooperated with the Navy's directions to stop, lower their ladder, and allow a boarding team (BT) to embark. Unfortunately, too many vessels are considered non-compliant. This situation requires the VBSS BT to travel alongside the vessel in a RHIB, and utilize grappling hooks attached to rope ladders in order to board it. As the BT reaches the deck, it quickly uses tactics to secure it and the pilothouse. The next phase in the operation is to conduct a search throughout the remainder of the vessel (Nguyen & Baker, 2012).

Rank (2012) found that historically, the U.S. Navy has utilized some form of VBSS tactics from its creation. A few crewmembers were chosen to focus primarily on combat during the Revolutionary War that ultimately developed into the Marine Corp. These marines were vital when large ship battles transitioned into close combat situations (Rank, 2012). Vann (2012) research shows that as the challenges and threats in the maritime environment evolve, the technological advancements, tactics, and policies have adapted to meet those requirements. Until recently, the use of VBSS was reserved for conducting maritime interdiction operations, and was seen as a secondary focus on enhancing the United States Navy's primary objectives of protecting sea lines of communication from entities that threaten them. Initially, minimal training was offered to ship crewmembers that volunteered to conduct boarding missions that were generally never conducted, or focused more on rescue and assistance of small vessels under duress (Vann, 2012). Today, MIO has been transitioned from a secondary mission, and added to the list of priorities for the Navy's surface fleet.

2. Communication as a Challenge

The challenges that VBSS teams face are numerous; therefore, the purpose of this thesis is to focus specifically on how communications can hinder the effectiveness of BT missions. The main challenges that will be addressed concern the environment in which VBSS teams operate; the communication gaps that are inherent to the team; and the increased demand on communication throughout.

a. Environment

The maritime environment in itself creates unique challenges for effective communications. The distance required for maintaining communications occasionally limits the tactical choices of the controlling ship or operational commander. If the controlling ship decides to maintain a distance beyond the line-of-sight (LOS) of the vessel of interest (VOI), additional communication elements must be put into place for reach-back connectivity. This ability to reach-back diminishes as distance between the command ship and the VBSS team increases.

Edelkind (2012) also explains that the VOI also creates a challenge for VBSS teams to communicate both with elements outside of the vessel and among team members below decks. The metal that most vessels are built from create characteristics of a Faraday cage. This is especially true of the much larger freighter vessels. The series of metal compartments within the vessel dampen radio waves, and interrupt communication signals. This effect increases as a team member descends further into the ship; therefore, increasing the likelihood that communications will be disrupted (Edelkind, 2012).

b. Communication Gaps

As explained by Edelkind (2012), an extension of environmental challenges is the gap in communications that are inherently created once a boarding team enters a vessel. These gaps can be detrimental to the success of any VBSS mission without a network able to provide continuous communication capabilities. The mesh network topology has been introduced as a possible solution to meet the communication challenges. The challenge is to maintain Internet protocol data flow between the control vessel and the boarding team throughout the mission, and the command and control (C2) capabilities for commanders. The lack of a data transfer capabilities within the network prevents vital mission information to flow from the mission commander to the VBSS team such as surveillance data or from the team to the mission commander such as intelligence about the VOI. Some theaters require that any intelligence derived from a VOI must be completed within an hour; therefore, mission commanders expend a great amount of resources to maintain that communication capability (Edelkind, 2012). In 2012, Vann’s study explained that the conservation of time and resources allocated for a VBSS mission is extremely important to both the control ship and the VOI. For example, fuel costs and delayed shipments damage the shipping company that owns the VOI, and the time spent by VBSS teams searching innocent vessels prevents them from addressing other possible maritime threats (Vann, 2012).

Presently, the Navy does not have an easy and robust communications platform able to provide real-time intelligence throughout the boarding team as it conducts its mission. As explained by Sundall (2008), the vessels themselves hinder communications between boarding members as they travel through the VOI. This is an obvious safety concern for the team because any lag in operational responsiveness to identified threats can mean the difference between life and death. Creating a network to cover this gap will enable individual team members to take action on true and timely intelligence (Sundall, 2008).

c. Data Requirements

Stavroulakis (2006) shows that the current VBSS procedures are not able to conserve critical time in regards to gathering and transmitting important mission data, and many different means of communicating data are required for boardings. These forms range from regulated text and voice transfers to the physical delivery of intelligence derived from team members below decks. This causes a disconnection between the boarding officer and the controlling ship, which results in less informed decision making (Stavroulakis, 2006).

Sundall (2008) research explains that VBSS missions have evolved into highly complex missions that require careful planning and extensive coordination among all elements involved. No longer are traditional communications capabilities a sufficient means to conduct such operations. New means of transferring intelligence data is needed when requirements on boarding teams increase. For example, a team may need to transmit a video stream or photos of the inner portion of the ship’s hull and machinery. These relatively new intelligence requirements placed on VBSS teams are a great asset, but place an enormous burden on the communication links needed for effectiveness (Sundall, 2008).

Stavroulakis (2006) also explains that most VBSS teams are stand-alone units on a VOI that are linked to a shore-based or ship-based supporting element. This communication link does not match the needs of the boarding team as it conducts its mission. The teams are highly trained law enforcement or military units, but still require their outside connect to insure that their findings are correctly evaluated, and verified for authenticity. As a result, much of the data gathered from the VOI is processed external to the boarding team. In addition, due to the time restraints placed on the average boarding operation, the information must be as near to real-time as possible (Stavroulakis, 2006). So not only are there requirements for more data to be transferred, but it must be accomplished with even greater speeds.

The common factor among the different applications of VBSS operations is that the boarding team's situational awareness suffers due to a lack in information flow and communication equipment capabilities. This hinders the requirement to make timely and effective decisions when necessary (Stavroulakis, 2006).

Therefore, it is vital that VBSS teams have the ability to communicate reliably among themselves, and to the supporting elements in the operation. This thesis will propose the use of communication devices that are capable of forming ad-hoc wireless mesh networks that provide that robust and reliable means of transferring near real-time data to and from VBSS teams.

B. MESH NETWORKS

A wireless mesh network (WMN) is a network that wirelessly applies multi-hop communications technology for forwarding traffic to and from wired entry points for Internet access (Bruno, Conti, & Gregori, 2005).

Motorola (2006) describes the components of a mesh network as nodes, and can be comprised of the stationary sections of infrastructure or mobile units within the network itself. This forms a decentralized broadband network that only requires each node to transmit to an adjacent node instead of the eventual communication endpoint (Motorola, 2006). In 2005, Motorola showed that this is possible due to the node's ability to operate as router/repeaters when transmitting data, and allows the network to spread across greater distances while maintaining high data rates, and connecting non-line-of-sight (NLOS) users throughout challenging environments (Motorola, 2005).

By acting as routers and repeaters, Jun and Sichitiu (2003) explain that the nodes allow data packets to be forwarded to the gateways that are connected to the Internet, and out of transmission range of isolated nodes. The network is then able to self-organize and self-configure connections to automatically create and maintain transmission routes dynamically among each node. (Jun & Sichitiu, 2003).

Motorola (2005) explains another important point to make, which is that WMN is not the introduction of new radio technologies or signal modulations, but a new way to construct networks with current radio technologies. The emphasis is on the network architecture rather than any specific radios within the network. The network architecture is comprised of the mesh components, their structure, and how they interact with each other, while radio modulation focuses on how data is transmitted and received by specific radios. Therefore, mesh networking allows current radios to leverage their technology, and be applied to virtually any radio scheme needed for the environment (Motorola, 2005).

1. Types of Mesh Networks:

WMNs can be constructed in three basic architectural schemas: infrastructure, client, and hybrid meshing. Any combination of the three can be applied to capture the maximum benefits of meshing different networks within an environment (Mesh Networks, 2013).

a. Infrastructure Networks

Infrastructure meshing creates a wireless backhaul mesh that uses wired access points and wireless routers to reduce costs as well as increase network coverage and reliability (Mesh Networks, 2013). Djohara, Hafid, and Gendreau explain that the access points offer Internet access to mesh clients by using the multi-hop concept of forwarding data to the mesh routers also known as relays. This is accomplished until a mesh gateway is reached. The mesh gateways act as bridges to connect the established wireless infrastructure and the Internet (Djohara et al., 2012). This approach provides a backbone for conventional clients and enables the integration of new WMNs with existing wireless networks utilizing the gateway or bridge functionalities in mesh routers (Akyilidiz & Wang, 2005).

(1) Backhaul. Backhaul is the service of forwarding data that originates from a user's device along the wireless backbone, and distributed out to an external network or Internet connection (Bruno et al., 2005).

(2) Backbone. Backbone is a series of wireless connections that forms the core of the mesh, and provides transparent routing to and from a traditional wired backbone that allows for Internet connectivity (Bruno et al., 2005). See Figure 1.

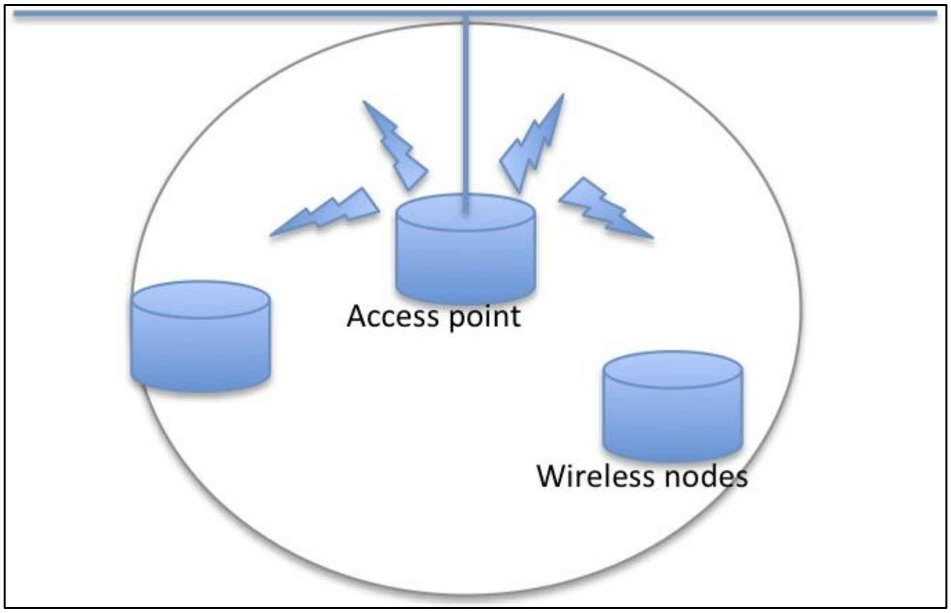


Figure 1. Infrastructure Topology (after Dean, 2013, p. 299)

b. Client Networks

Client meshing provides wireless peer-to-peer networks to form throughout the client devices within the WMN, and alleviates the need for any existing network infrastructure to be present (Mesh Networks, 2013). Akyilidiz and Wang (2005) add by explaining that this type of architecture allows the client to perform the required routing, configuring, and end user applications, eliminating the need for mesh routers. Client WMNs are usually created using a single type of radio or device, which makes them ideal for creating, diversified conventional ad hoc networks in difficult wireless environments (Akyilidiz & Wang, 2005). Jun and Sichitiu (2003) expounds that the traffic pattern is the main difference between WMNs and an ad hoc network. The traffic is passed either to or from a gateway in WMNs, while ad hoc networks allow the traffic to flow between indiscriminate pairs of nodes (Jun & Sichitiu, 2003). Since WMNs self-organize and self-configure dynamically, the creation and maintenance of ad hoc networks is automatic (Akyilidiz & Wang, 2005).

(1) Ad Hoc Networks. As talked about by Bruno et al. (2005), an Ad Hoc Networks are also known as mobile ad hoc networks (MANETs), which is a cluster of mobile nodes connecting with each other through a wireless medium where nodes can easily and dynamically self organize into ad hoc network topologies. This creates a seamless integration of devices to allow users Internet access in environments without existing communication infrastructure. These environments are most notably in disaster relief scenarios or battlefield environments that consistently utilize the paradigm of ad hoc networks (Bruno et al., 2005). See Figure 2.

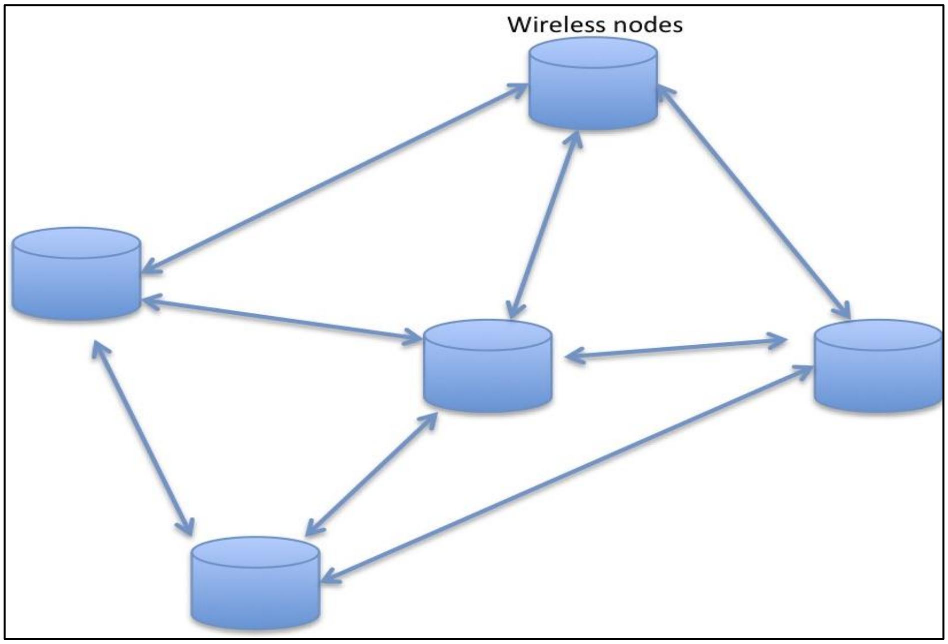


Figure 2. Ad Hoc Topology (after Dean, 2013, p. 298)

c. *Hybrid Networks*

Akyilidiz & Wang (2005) says that the hybrid network architecture combines the network models infrastructure and client meshing where clients can use mesh routers, and directly integrate with other established mesh networks. The infrastructure portion delivers connectivity to other services such as the Internet, Wi-Fi, cellular, and sensor networks, and the individual routing capabilities of network clients provide superior connectivity and coverage within the WMNs (Akyilidiz & Wang, 2005).

2. Advantages of Mesh Networks

WMN technologies have become a cornerstone for future generations of wireless networking. The recognition of the advantages of mesh networks over other wireless networks is driving researchers to develop new and innovative applications that capitalize on these benefits (Akyilidiz & Wang, 2005). The following text describes a variety of advantages that WMNs provide.

a. Reliability and Robustness

Bruno et al. (2005) states that for each pair of endpoints in the network, the wireless backbone establishes redundant paths to transmit data between them. This eliminates single points of failure within the mesh network, and significantly increases the reliability of communications (Bruno et al., 2005). Mesh Network (2013) shows that this self-forming and self-healing technique of using the routing intelligence of the nodes allows clients to spread out between access points, and removes potential network bottlenecks, which potentially improves the overall network’s performance. The network’s robustness against communication faults is also improved by this mesh architecture because it introduces multiple destinations and various routes for network clients to pass data. If certain access points are congested or have failed, the client can choose alternate paths to transfer data, thus ensuring the integrity of the network (Mesh Network, 2013).

b. Non-Line of Sight and Congestion Mitigation

The hopping of transmissions between adjacent nodes not only alleviates network congestion, but also enables nodes to reroute transmission around obstacles (Mesh

Network, 2013). By retaining the ability to circumvent environmental obstacles, it provides a line-of-sight (LOS) capability to users without direct LOS links to each other (Djohara et al., 2012).

c. Lower Infrastructure and Operational Costs

Jun and Sichitiu (2003) evaluates that the initial investment costs to establish a mesh network infrastructure are minimal because each node device within the network can be introduced incrementally as needed, and as nodes are added, the overall network's coverage and reliability increases. The same is true for network gateways, which can be added as needed. Since the mesh structure ensures the network contains multiple paths for each node to transmit data through the network, the same is true for gateways. If one gateway fails, other gateways in the network will absorb the network impact, and depending on the extent of the existing traffic load, only a slight reduction of overall network performance will be noticed by users (Jun & Sichitiu, 2003).

Motorola (2005) shows that the backhaul requirements for a mesh network are typically less than traditional wireless networks. This reduces the cost of deploying and operating the network in new environments. The self-healing and self-forming feature of mesh networks also helps lower administration and maintenance costs. It lowers these costs by reducing the network administration skill sets, and eliminating the need for 24-hour maintenance support, both required of most centralized wireless networks (Motorola, 2005).

d. Reduced Power and Spectrum Requirements

Basic physics dictates the transmit power output requirements of data rate and the radio transmission range between any wireless network endpoints. As illustrated in Figure 3, for any radio modulation or protocol, the data rate or throughput will decrease as the range from the transmitter increases; the output power from the transmitter must increase in order to maintain the connection. If the output power has already reached its limit, data packets will begin dropping.

$$\boxed{C = B\log_2\left(1+\frac{S}{N}\right)}$$

Figure 3. Shannon’s capacity equation (from Centers, 2013)

Mesh Networks (2013) explains that by hopping through the chain of adjacent nodes, mesh networks provide longer ranging capabilities between endpoints, while maintaining optimal data rates. Each node acts as a transmitter and receiver, therefore, the relative distance for transmissions are much shorter. By shortening this distance, the transmit power required for connectivity is also lowered, which in turn lowers the networks overall power requirements. This develops into connections that can support the potentially high downlink and uplink data rates over greater distances. This also reduces network frequency interferences, and allows for residual spectrum reallocation for other users. Simply stated, WMNs allow for greater throughput over longer distances by leveraging the physics of radio frequency (RF) properties (Mesh Networks, 2013).

As shown in Mesh Networks (2013), leveraging the routing capabilities of WMN technologies, many of the world’s largest mobile networks are adapting to the techniques primarily created for communication in battlefield environments. The redundancy of the mesh network construct assists military strategists by pushing intelligence and decision making to the tactical edge of the network (Mesh Networks, 2013). Many industrial developers are meeting this growing demand of wireless mesh applications by creating proprietary software communication devices that establish WMNs capabilities in a multitude of environments (Bruno et al., 2005).

C. OPERATING MESH NETWORKS

1. Network Management System

As defined by Dean (2013), a network management system (NMS) is a general term referencing the assessment, monitoring, and maintenance of every aspect of a network. It includes techniques that check for hardware faults, important applications’ quality of service (QOS), providing records of network assets and software configurations, and even determining the best time to conduct system upgrades. The network's size and importance determines the scale of NMS techniques needed. For example, a large network administrator might run continual network management applications to check connections and devices for correct performance within set thresholds. A device that does not respond within the given performance parameters, the application monitoring that device will send an alarm to the responsible administrator. For smaller networks, the economic feasibility for a comprehensive NMS might not be worth the investment. Instead, an application designed to periodically test devices and connections for functionality would be a better fit (Dean, 2013).

2. FCAPS

To effectively manage all aspects of a communication network, many tools are required. The OSI management model categorizes required functionalities into five distinct areas called FCAPS. These functional areas are as follows:

- Fault management
- Accounting management
- Configuration management
- Performance management
- Security management. (Bieszad, Paqurek, & White, 2009)

Subramanian (2011) explains that the networks consist of routers, switches, and hubs that are connected through various network links. Servers and workstations are connected locally within each network. All require various technologies for network management, but the primary focus is generally on the health and performances of routers, switches, the links, and servers (Subramanian, 2011).

Subramanian (2011) states that configuration management is the first step in managing the network. This step identifies the configuration and topology desired for the network elements, their agents, and the NMS itself. From this framework, the other management tools can be adapted into the NMS construct, and management requirements identified (Subramanian, 2011).

Subramanian (2011) describes the Fault management functionality provides the NMS with the capability to support monitoring of the health of network elements and their links. Alarms are generated based on desired thresholds defined by network administrators. Depending on the nature, severity, and importance of the fault, a variety of notifications can be generated for information. Fault notifications can be constructed to assist managers in quickly identifying areas of the network that can be proactively mitigated (Subramanian, 2011).

Subramanian (2011) states that performance management is another important functional tool for network administrators. The NMS utilizes this function to provide managers with information they can quickly gauge how well network elements and the network as a whole is performing. Planning and management reports can be generated in order to keep upper-level supervisors informed on the network status such as: network availability, system availability, problem reports, service response to problems, and customer satisfaction. Trend reports can also support administrators to monitor traffic patterns both internal and external to the network, and identify bottlenecks in traffic flow. The administrator can take corrective actions, such as re-routing traffic or changing priorities in the different classes of traffic in order to alleviate the problem areas. Performance reports can also be used to determine long-term traffic trends that help administrators plan effective means to improve upon future network expansions (Subramanian, 2011).

Subramanian (2011) describes the least developed of the network management functions is the accounting management application. Accounting management includes the capturing of individual host use, administrative segments, and external traffic. This allows network managers to identify possible hidden costs by elements requiring significant resources (Subramanian, 2011).

Subramanian (2011) Explains that security management is an issue that is both technical and administrative. This application provides security for network access, and the information that flows to and from outside sources to include Internet connections. It also monitors data storage, and the manipulation of that data as it travels within the network. It is also important that the security management covers the NMS as well. The

NMS database often contains confidential information about the organization that needs to be restricted to authorized personnel. The NMS also provides the means in which the network elements can be reconfigured, which needs to be carefully controlled, and access restricted (Subramanian, 2011).

Network management involves the complete FCAPS spectrum of application functions. Configuration, fault, and performance management are found in almost every network management deployment. In some cases, the NMS is also used for security and accounting management (Subramanian, 2011, pp. 361–364).

3. MIBs

Dean (2013) states that a managed network device can be comprised of several objects that include processors, memory, hard disks, or intangibles such as network performance and utilization. For example, an agent can manage a server to see how many users are on at any given time and at what capacity the processors are working at. The definitions of the network devices and their collected data are gathered in a management information base (MIB) (Dean, 2013, p. 701).

As described in IEEE (2012), the MIB is a database used by both an agent and the management processes to manage entities in a network, and to store and exchange management information. There are two basic forms of MIBs, the agent MIB and the manager MIB. The agent MIB consists of local network information that an agent needs to process. The manager MIB compiles the information of all network devices that it manages. (Subramanian, 2011, p. 102) The database is a hierarchical tree structure where at each level the entry is assigned by an object identifier (OID), and is designated by various organizations. The upper level of the MIB tree lists the OIDs assigned by technology standards generated by organizations, and the lower level OIDs are derived from the associated organizations specifying its particular need. The hierarchical model allows for higher-level network management, and the extension to more specific areas such as databases and email (IEEE, 2012).

4. RFCs

As explained by Alvestrand (2004) request for comments (RFC) are published by the Internet Engineering Task Force (IETF) and the Internet Society who are the primary technical standards developing organizations for the Internet. An RFC describe methods, behaviors, research, or innovations associated with the Internet as a whole as well as the systems connected to it. Engineers and computer scientists submit their memoranda for peer review or to communicate new technology concepts. The IETF will then decide on which proposed RFC could be adopted as Internet standards. The original RFCs were simple unofficial messages invented by Steve Crocker, and were used to document problems and solutions during the development of ARPANET. RFCs have evolves into official Internet documents describing specifications, communication protocols, procedures, and events (Alvestrand, 2004).

Dean (2013) discusses that as some RFCs are considered industry standards, some are not. Therefore, two special subseries were developed within RFCs to distinguish between Internet standards and non-standards. The subseries are called For Your Information (FYI) and Standard (STD) RFCs. The FYI RFCs are developed by individual service groups within the IETF to document useful information, and the STD RFC identifies the RFCs that have been reviewed and released as Internet standards. Each RFC is assigned an RFC number that is indexed for easy retrieval including FYIs and STDs. As FYIs or STDs are revised, the RFC number will change, but the FYI and STD number will not. This assists new Internet users to reference helpful informational documents (Dean, 2013, p. 135).

5. RMON

As explained by Subramanian (2011), every packet of information traveling between a manager and an agent can be opened and analyzed without disrupting the communication flow. This is known as monitoring or probing the network. The device that is used for this function is called a network monitor or probe. This information that is gathered and analyzed locally can be transmitted to a remote NMS for monitoring. The remote monitoring using a probe is known as remote network monitoring (RMON).

Using RMON devices offers several advantages. The first advantage is that each RMON device monitors and evaluates the network segments locally. This information is transmitted to the NMS in solicited and unsolicited forms. For example, when the RMPN device monitors a local network element and it detects an issue, it sends an alarm to the NMS. Due to the localized monitoring, the data is more reliable. This also reduces traffic loads on the network. Another advantage of monitoring locally using RMON is that it provides the manager performance statistics that are more accurate, and gives the manager greater control over the network. This is due to the ability of RMON devices' monitoring in a continuous nature. Overall, the benefits of RMON technology is that users receive higher network availability, and administrators see greater productivity (Subramanian, 2011, pp. 288-289).

6. Software Defined Radios

Within the scope of this thesis, the monitoring of a wireless mesh network between an on scene operator and the command and control element supporting VBSS teams during MIO, it is important to discuss the commercial-off-the-shelf (COTS) technologies that will be utilized within the experiment. This COTS technology is software-defined radios (SDR).

SDR is an architecture that is flexible and applicable to a variety of radio standards. The term software radio was created by Joseph Mitola (1999) to officially mark the shift from digital radio to multiband and multimode SDRs. This architecture is widely applicable to trunk radios, peer networks, and mobile military communication systems. (Mitola, 1999) Tabassum, Kalsait, and Suleman (2011) states that the SDR communication system is still limited within the radio frequency (RF) portion of the frequency spectrum, but allows control for a variety of options. Examples of these options are multiple modulation methods, filtering, wideband or narrowband operations, and spread spectrum techniques (Tabassum, Kalsait, & Suleman, 2011). All of these are possible assets to incorporate into a MIO VBSS communication network.

Mitola (1999) emphasizes that it is also important to note that SDRs do not just transmit information. It is able to characterize the transmission channels available, finds the propagation path, and builds the correct channel modulation in order to transmit. It also does not just receive information. The radio identifies the mode of the incoming transmission, and adaptively removes interference. It then calculates and combines the properties of desired signal in order to decode the modulated channel. Finally, it removes residual errors to receive the signal with lowest possible bit error rate (BER) (Mitola, 1999).

THIS PAGE INTENTIONALLY LEFT BLANK

III. EXPERIMENTAL STUDY OF PROTOTYPE NETWORK

The following experiments were conducted to test the abilities of COTS communication equipment as they apply to a VBSS mission in a MIO environment. This chapter details these experiments and analyzes the performances of both WaveRelay (WR) and Trellisware (TW) radios in a mesh network, and associated monitoring software.

A. TESTING CRITERIA

The U.S. Coast Guard (USCG) tasked Naval Post Graduate students with the challenge of creating a WMN that could withstand the dynamic environment the VBSS BTs operate in during MIO. The following criteria were given as crucial factors for performance needs during these missions.

1. Voice and Data Communications from a USCG Cutter to BT Members Located within a Large Freighter

- Continuous
- Reliable
- Secure

2. Management of Communication Network

- Ability to track all nodes within the network
- Data and voice performance monitoring
- Throughput analysis
- Fault identification and remedy
- Configuration management

B. INFRASTRUCTURE USED

In order to meet the USCG communication challenge, this section will identify the environments chosen for the experiment, and the associated technologies involved for each.

1. Environment

In the San Francisco Bay area, two locations provided the opportunity to recreate the environments in which VBSS BTs conduct operations. The first was aboard the *SS Jeremiah O'Brien (SS O'Brien)* and the second aboard the *Admiral W.M. Callaghan* (*ADM. Callaghan*). Both will be described below.

a. SS Jeremiah O'Brien

The *SS O'Brien* was a World War II liberty ship that provides 450 feet of metal infrastructure divided into a multitude of compartments, and separated by watertight hatches. The properties of the metal design provide reflective surfaces and possible interferences the recreate a sufficient environment for WMN testing. The (WR) communication equipment will be used to construct the WMN on this ship (The National Liberty Ship Memorial, 2014).

b. ADM. W. M. Callaghan

As described by NavSource (2014), the *ADM. Callaghan* is a cargo ship designed to transport large vehicles. It is comprised completely of metal, and over 694 feet in length. The interior is an open bay concept with sloping ramps connecting large cargo holds on each deck. This ship was chosen not only for the metal properties, but also for the size. It is assumed that the larger ship size will allow the WMN nodes extend farther apart in order to fully test the communication equipment's capabilities. The TW communication equipment will be used to construct the WMN on this ship (NavSource, 2014).

2. Communication Equipment

The communication equipment chosen for this experiment are comprised of two different proprietary commercial SDRs.

a. WaveRelay Systems

A development of Persistent Systems, the WR system was designed as a commercial solution for communications on the move (COTM) systems. It operates on the OSI Data Link Layer 2 providing data, video, and voice for a scalable peer-to-peer network that is portable, and easily integrated with other Layer 2 devices. WR systems provide a secure web management interface that contains network management capabilities and configuration functionality. For the experiment, the Man Portable Unit Third Generation (MPU3) and Fourth Generation (MPU4) systems were used to develop the WMN topology on the *SS O'Brien*. Photos and specifications of the WR MPU3 and MPU4 is shown in Figures 4 and 5 respectively.

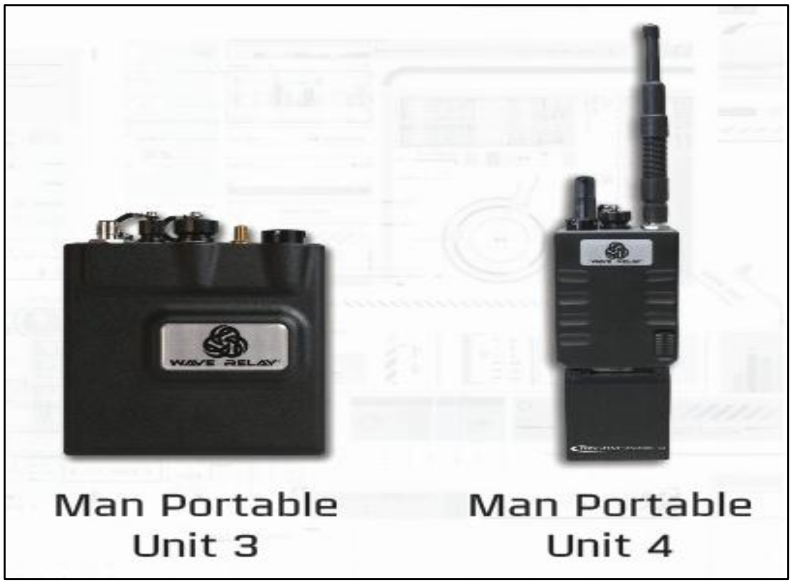
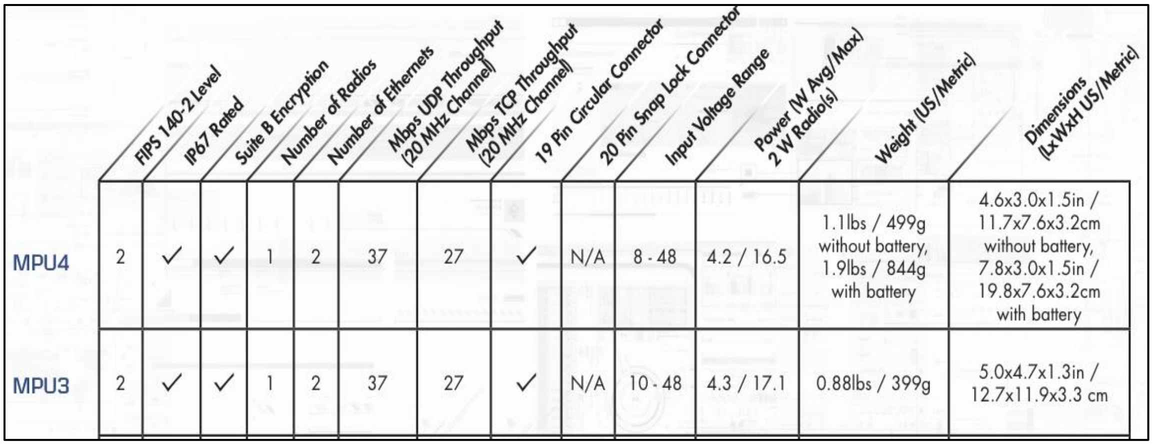


Figure 4. WaveRelay MPU3 and MPU4 (after Persistent Systems, 2013)



	FIPS 140-2 Level	IP67 Rated	Suite B Encryption	Number of Radios	Number of Ethernets	Mbps UDP Throughput (20 MHz Channel)	Mbps TCP Throughput (20 MHz Channel)	19 Pin Circular Connector	20 Pin Snap Lock Connector	Input Voltage Range	Power (W Avg/Max) 2 W Radio(s)	Weight (US/Metric)	Dimensions (LxWxH US/Metric)
MPU4	2	✓	✓	1	2	37	27	✓	N/A	8 - 48	4.2 / 16.5	1.1lbs / 499g without battery, 1.9lbs / 844g with battery	4.6x3.0x1.5in / 11.7x7.6x3.2cm without battery, 7.8x3.0x1.5in / 19.8x7.6x3.2cm with battery
MPU3	2	✓	✓	1	2	37	27	✓	N/A	10 - 48	4.3 / 17.1	0.88lbs / 399g	5.0x4.7x1.3in / 12.7x11.9x3.3 cm

Figure 5. WaveRelay MPU3 and MPU4 specifications (after Persistent Systems, 2013)

b. Trellisware Systems

The second commercial SDR that was chosen for the experimentation is the CheetahNet tactical network device designated the TW220. Built by TW Technologies Inc., the TW220 was specifically designed to form ad hoc WMNs in a variety of environments including MIO. Also a Layer 3 device, it provides sufficient scalability, and automatically establishes a WMN once other devices are introduced to the network. These devices are to be used to establish a manageable WMN on board the *ADM. Callaghan*, and provide data for analysis. A photo and specification's list are provided in Figures 6 and 7 (Trellisware, 2014).

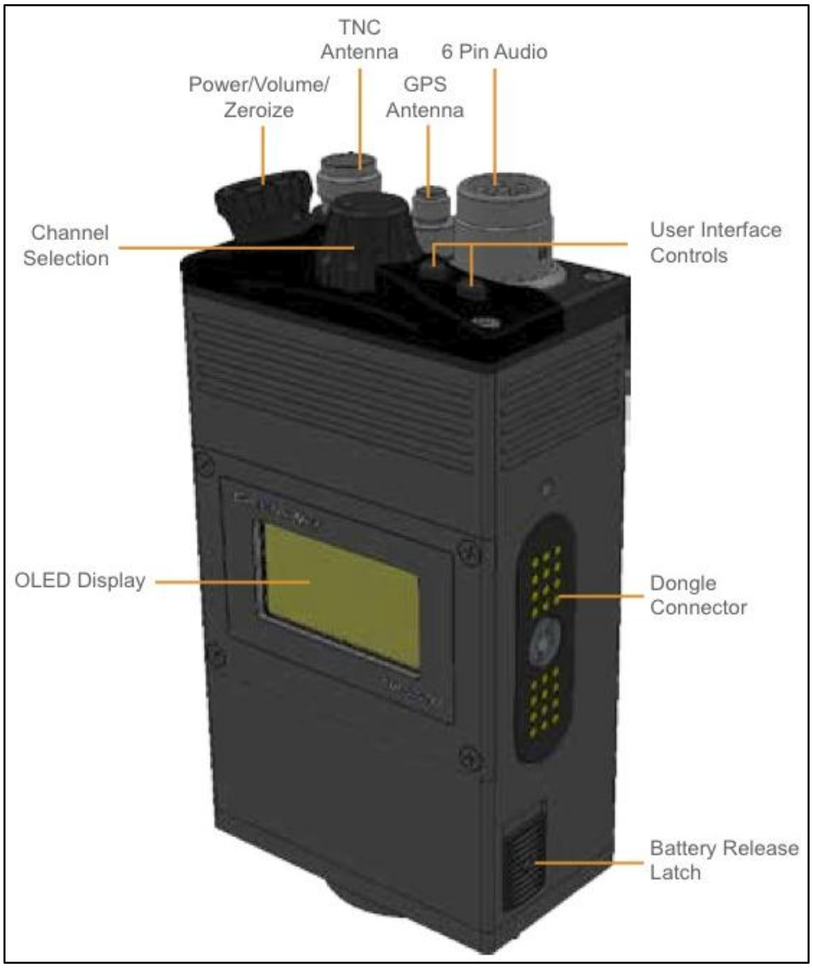
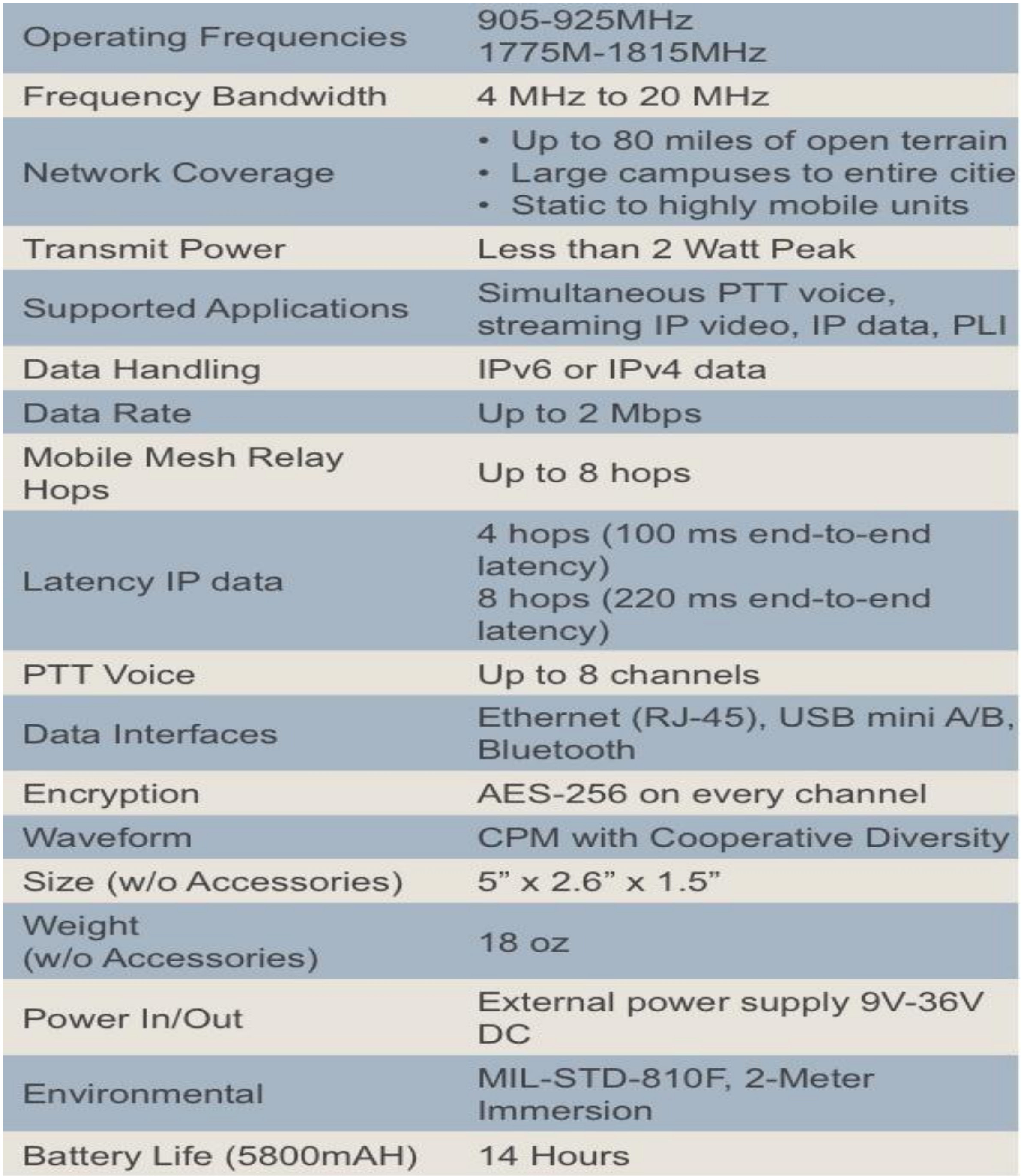


Figure 6. TW220 (after Trellisware, 2014)



Operating Frequencies	905-925MHz 1775M-1815MHz
Frequency Bandwidth	4 MHz to 20 MHz
Network Coverage	• Up to 80 miles of open terrain • Large campuses to entire citie • Static to highly mobile units
Transmit Power	Less than 2 Watt Peak
Supported Applications	Simultaneous PTT voice, streaming IP video, IP data, PLI
Data Handling	IPv6 or IPv4 data
Data Rate	Up to 2 Mbps
Mobile Mesh Relay Hops	Up to 8 hops
Latency IP data	4 hops (100 ms end-to-end latency) 8 hops (220 ms end-to-end latency)
PTT Voice	Up to 8 channels
Data Interfaces	Ethernet (RJ-45), USB mini A/B, Bluetooth
Encryption	AES-256 on every channel
Waveform	CPM with Cooperative Diversity
Size (w/o Accessories)	5” x 2.6” x 1.5”
Weight (w/o Accessories)	18 oz
Power In/Out	External power supply 9V-36V DC
Environmental	MIL-STD-810F, 2-Meter Immersion
Battery Life (5800mAH)	14 Hours

Figure 7. TW220 Specifications (after Trellisware, 2014)

3. NMS Requirements

The proprietary NMS utilized within the WR and TW radios is beneficial in getting an overall picture of the networks. However, the NMS suite will not provide us with all of the variables that we are interested in obtaining in this project. Therefore, to compensate for this, each MANET radio will have tertiary SNMP-enabled devices attached to them. Through these devices we will use the Solar Winds and QCheck NMS suites to have better insight into the operations of the network. The combination of utilizing the two different NMS suites will have significant value for this project. The following RFCs list shows the requirements determined to be the most useful when choosing the NMS suites.

- RFC 1757: Remote Network Monitoring Management
- RFC 3877: Alarm Management Framework
- RFC 2863: The Interfaces Group
- RFC 2925: Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup
- RFC 4022: Transmission Control Protocol
- RFC 4113: User Datagram Protocol
- RFC 4268: Entity State
- RFC 4293: Internet Protocol

C. EXPERIMENT DESIGN

This section will describe the experiment designs for both WMNs established on board the *SS O'Brien* and the *ADM. Callaghan*.

1. Wave Relay Design

Permission was granted to perform the BT to cutter experimentation onboard the historical WWII liberty ship *SS Jeremiah O'Brien* stationed at Pier 45 in San Francisco. Onboard the *SS O'Brien*, the experimental network was constructed IAW Appendix A. Five WR) wireless mesh nodes were physically located throughout the vessel. Two of the nodes were WR MPU-4s with Samsung devices attached to host a variety of IP-based applications. These nodes were utilized by the BTs to sweep the vessel in a simulated environment and also served as wireless access points. Two other WR nodes were utilized as access points and relays throughout the *SS O'Brien*. The final WR node (IP address whose final octet was .56) was utilized as the connection to the San Francisco police boat (SFPD) (.246). For the purposes of the experiment, the SFPD boat specifically portrayed the Network Operation Center (NOC) onboard a USCG cutter and had an experiment team member onboard for data collection and network monitoring purposes. The SFPD boat also acted as a relay connection between the *SS O'Brien* and the Golden Gate Bridge (GGB) WR node (.248). The GGB node had a VPN connection to Naval Postgraduate School CENETIX Lab (.41) network. The CENETIX Lab provided additional network monitoring tools and provided the experimentation team access to additional resources via the VPN connection.

For the purpose of the experiment, the management roles were divided into two separate locations. One team member was stationed onboard the notional USCG cutter NOC (SFPD boat) while the other two members were physically located on the boarded vessel (*SS O'Brien*). The USCG NOC member utilized a laptop equipped with SolarWinds network management software for fault, configuration, and performance monitoring. The USCG NOC member also utilized the WR proprietary web interface for other metrics that are not retrievable via the SolarWinds interface.

The two members onboard the SS O'Brien were purely used as liaisons between the BT members and the USCG NOC. As the USCG Cutter observed indications of faults, he would notify the liaisons for troubleshooting purposes. The liaisons onboard the SS *O'Brien* were also equipped with laptops that were connected wirelessly to the WR network. They were able to monitor the network in near real time via the WR proprietary web interface.

The decision support focus of our management process was to provide the status of applicable variables, or similar variables from NMS sources, in an easily understandable format to facilitate network management. Throughout the experiment, the NOC stationed onboard the USCG cutter was the focal point of the decision support system. As network status changed during the experiment, the testing member aboard the SFPD boat analyzed the results using multiple graphical representations and then provided feedback to the SS *O'Brien* through the use of the decision support software (Qcheck, SolarWinds, and WR).

2. Trellisware design

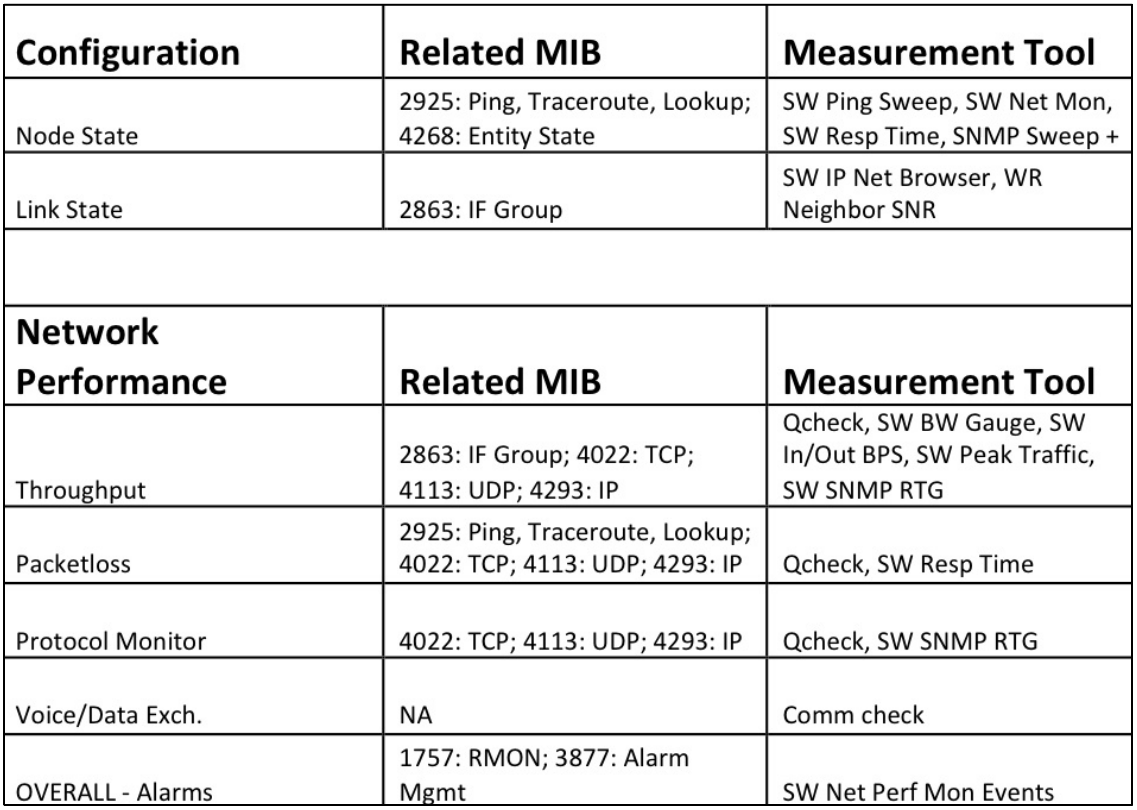
Permission was granted to perform the BT to cutter experimentation onboard the *ADM. Callaghan* stationed in Alameda Works Shipyard. Onboard the *ADM. Callaghan*, the WMN was constructed IAW Appendix B. Five TW CheetahNet TW220s were physically located throughout the vessel. Two of the devices were utilized as network endpoints attached to laptops. The remaining three devices were utilized by the BT to sweep the vessel in a simulated environment and served as access points and relays throughout the *ADM. Callaghan*.

For the purpose of the experiment, the management role was divided into two separate locations. One team member was stationed topside on the weather deck, and the other was located within the lower levels in order to maximize the distance between the two nodes. The topside node utilized a laptop equipped with SolarWinds and QCheck network management software for fault, configuration, and performance monitoring. The topside node also utilized the TW proprietary web interface for the remaining network management metrics.

The remaining three nodes onboard the *ADM. Callaghan* were used as network nodes between the two endpoints. They were to maneuver throughout the ship in order to expand the WMN, and report their locations. The topside node observed possible faults, and would capture screenshot data from the utilized NMSs in place.

IV. DATA ANALYSIS

Before deploying the two networks in San Francisco Bay and Alameda, both were set up at NPS in the CENETIX Lab to establish a baseline using data captures of SolarWinds, QCheck, and the proprietary web interfaces of WR and TW respectively. Table 1 depicts the specific configuration and network performance metrics that was obtained via a baseline configuration throughout the experiment.



Configuration	Related MIB	Measurement Tool
Node State	2925: Ping, Traceroute, Lookup; 4268: Entity State	SW Ping Sweep, SW Net Mon, SW Resp Time, SNMP Sweep +
Link State	2863: IF Group	SW IP Net Browser, WR Neighbor SNR
Network Performance	**Related MIB**	**Measurement Tool**
Throughput	2863: IF Group; 4022: TCP; 4113: UDP; 4293: IP	Qcheck, SW BW Gauge, SW In/Out BPS, SW Peak Traffic, SW SNMP RTG
Packetloss	2925: Ping, Traceroute, Lookup; 4022: TCP; 4113: UDP; 4293: IP	Qcheck, SW Resp Time
Protocol Monitor	4022: TCP; 4113: UDP; 4293: IP	Qcheck, SW SNMP RTG
Voice/Data Exch.	NA	Comm check
OVERALL - Alarms	1757: RMON; 3877: Alarm Mgmt	SW Net Perf Mon Events

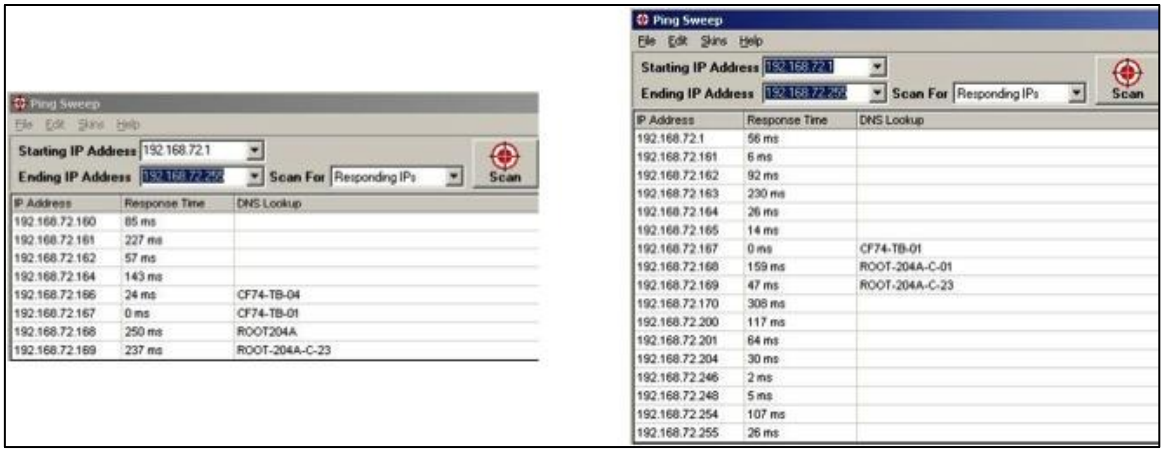
Table 1. Configuration and Network Performance Measurements (from Bartlett et al., 2013)

A. WAVE RELAY

This section will display and explain the data captured during the USCG Boarding Team to Cutter experiment onboard the *SS O'Brien*.

1. Node State

Figures 8 and 9 are the NMS data captures of both the baseline and execution showing the state of each node within the established WMN. The SolarWinds Ping Sweep probes the network to find existing nodes within a set IP range, and displays the nodes IP addresses and response times to the pings. The SolarWinds Network Monitor also displays the node's IP address and response time, but includes data for packet loss and node status. Node status shows the network manager whether a node is up or down in regards to its connection to the network.



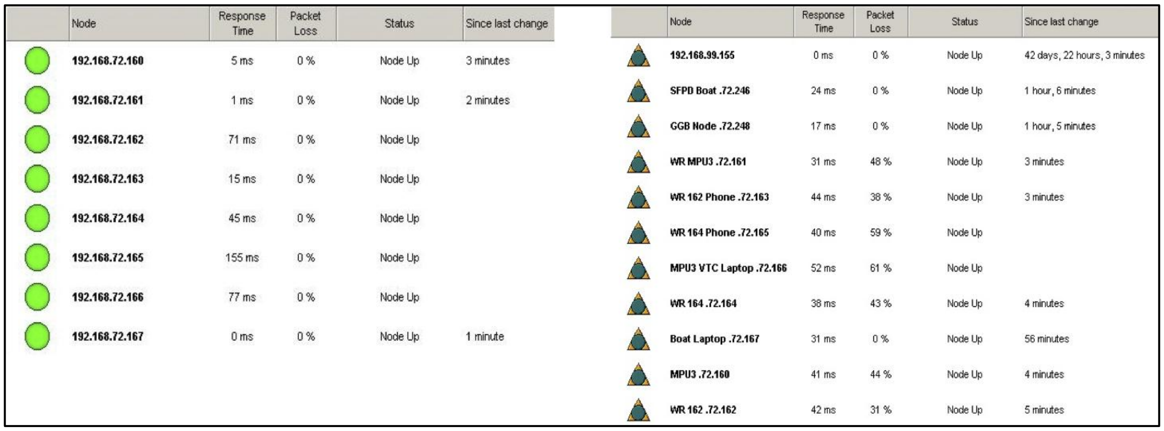
Starting IP Address 192.168.72.1
Ending IP Address 192.168.72.255
Scan For Responding IPs

IP Address	Response Time	DNS Lookup
192.168.72.160	85 ms	
192.168.72.161	227 ms	
192.168.72.162	57 ms	
192.168.72.164	143 ms	
192.168.72.166	24 ms	CF74-TB-04
192.168.72.167	0 ms	CF74-TB-01
192.168.72.168	250 ms	ROOT204A
192.168.72.169	237 ms	ROOT-204A-C-23

Starting IP Address 192.168.72.1
Ending IP Address 192.168.72.255
Scan For Responding IPs

IP Address	Response Time	DNS Lookup
192.168.72.1	56 ms	
192.168.72.161	6 ms	
192.168.72.162	92 ms	
192.168.72.163	230 ms	
192.168.72.164	26 ms	
192.168.72.165	14 ms	
192.168.72.167	0 ms	CF74-TB-01
192.168.72.168	159 ms	ROOT-204A-C-01
192.168.72.169	47 ms	ROOT-204A-C-23
192.168.72.170	308 ms	
192.168.72.200	117 ms	
192.168.72.201	64 ms	
192.168.72.204	30 ms	
192.168.72.246	2 ms	
192.168.72.248	5 ms	
192.168.72.254	107 ms	
192.168.72.255	26 ms	

Figure 8. SolarWinds Ping Sweep



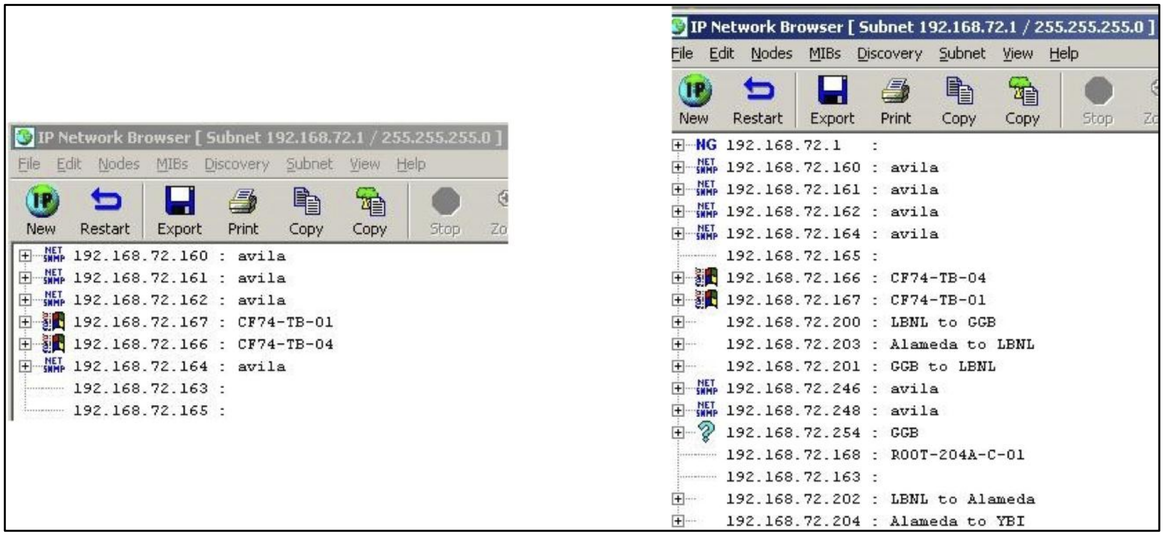
	Node	Response Time	Packet Loss	Status	Since last change
●	192.168.72.160	5 ms	0 %	Node Up	3 minutes
●	192.168.72.161	1 ms	0 %	Node Up	2 minutes
●	192.168.72.162	71 ms	0 %	Node Up	
●	192.168.72.163	15 ms	0 %	Node Up	
●	192.168.72.164	45 ms	0 %	Node Up	
●	192.168.72.165	155 ms	0 %	Node Up	
●	192.168.72.166	77 ms	0 %	Node Up	
●	192.168.72.167	0 ms	0 %	Node Up	1 minute

	Node	Response Time	Packet Loss	Status	Since last change
▲	192.168.99.155	0 ms	0 %	Node Up	42 days, 22 hours, 3 minutes
▲	SFPD Boat .72.246	24 ms	0 %	Node Up	1 hour, 6 minutes
▲	GGB Node .72.248	17 ms	0 %	Node Up	1 hour, 5 minutes
▲	WR MPU3 .72.161	31 ms	48 %	Node Up	3 minutes
▲	WR 162 Phone .72.163	44 ms	38 %	Node Up	3 minutes
▲	WR 164 Phone .72.165	40 ms	59 %	Node Up	
▲	MPU3 VTC Laptop .72.166	52 ms	61 %	Node Up	
▲	WR 164 .72.164	38 ms	43 %	Node Up	4 minutes
▲	Boat Laptop .72.167	31 ms	0 %	Node Up	56 minutes
▲	MPU3 .72.160	41 ms	44 %	Node Up	4 minutes
▲	WR 162 .72.162	42 ms	31 %	Node Up	5 minutes

Figure 9. SolarWinds Network Monitor

2. Link State

Figure 10 is the NMS data capture using the SolarWinds IP Net Browser application. This was an attempt to map the network's links of both the baseline and execution. The WR devices are layer 2 devices; therefore, the NMS was unable to diagram the network topology other than the two endpoints of the network.


IP Network Browser [Subnet 192.168.72.1 / 255.255.255.0]
File Edit Nodes MIBs Discovery Subnet View Help
New
Restart
Export
Print
Copy
Copy
Stop
Zo
IP Network Browser [Subnet 192.168.72.1 / 255.255.255.0]
File Edit Nodes MIBs Discovery Subnet View Help
New
Restart
Export
Print
Copy
Copy
Stop
Zo

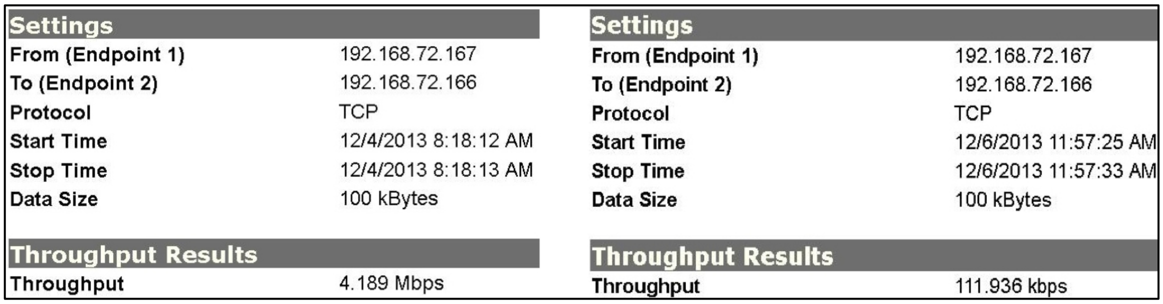
```
192.168.72.160 : avila
192.168.72.161 : avila
192.168.72.162 : avila
192.168.72.167 : CF74-TB-01
192.168.72.166 : CF74-TB-04
192.168.72.164 : avila
192.168.72.163 :
192.168.72.165 :
```

```
NG 192.168.72.1   :
192.168.72.160 : avila
192.168.72.161 : avila
192.168.72.162 : avila
192.168.72.164 : avila
192.168.72.165 :
192.168.72.166 : CF74-TB-04
192.168.72.167 : CF74-TB-01
192.168.72.200 : LBNL to GGB
192.168.72.203 : Alameda to LBNL
192.168.72.201 : GGB to LBNL
192.168.72.246 : avila
192.168.72.248 : avila
192.168.72.254 : GGB
192.168.72.168 : ROOT-204A-C-01
192.168.72.163 :
192.168.72.202 : LBNL to Alameda
192.168.72.204 : Alameda to YBI
```

Figure 10. SolarWinds IP Net Browser

3. Throughput

Figures 11 and 12 depict the throughput measurements. Both Qcheck and SolarWinds NMS were used to determine the amount of data that the network was moving from endpoint to endpoint. The baseline for each NMS indicates the throughput each network can obtain under ideal environments while the other shows the actual throughput when deployed.



Settings	
From (Endpoint 1)	192.168.72.167
To (Endpoint 2)	192.168.72.166
Protocol	TCP
Start Time	12/4/2013 8:18:12 AM
Stop Time	12/4/2013 8:18:13 AM
Data Size	100 kBytes
Throughput Results	
Throughput	4.189 Mbps

Settings	
From (Endpoint 1)	192.168.72.167
To (Endpoint 2)	192.168.72.166
Protocol	TCP
Start Time	12/6/2013 11:57:25 AM
Stop Time	12/6/2013 11:57:33 AM
Data Size	100 kBytes
Throughput Results	
Throughput	111.936 kbps

Figure 11. Qcheck TCP Throughput

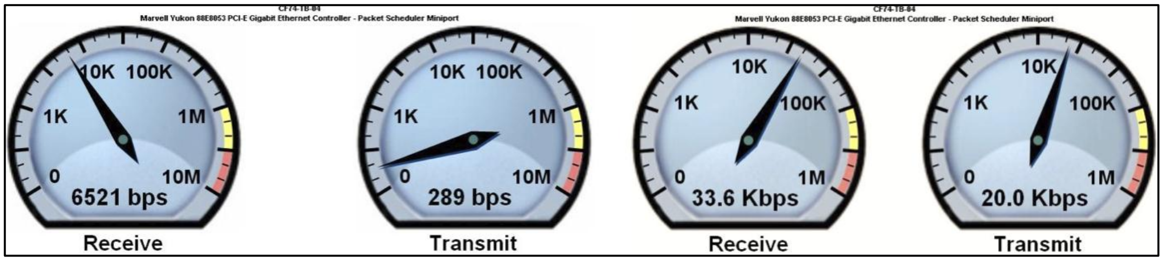
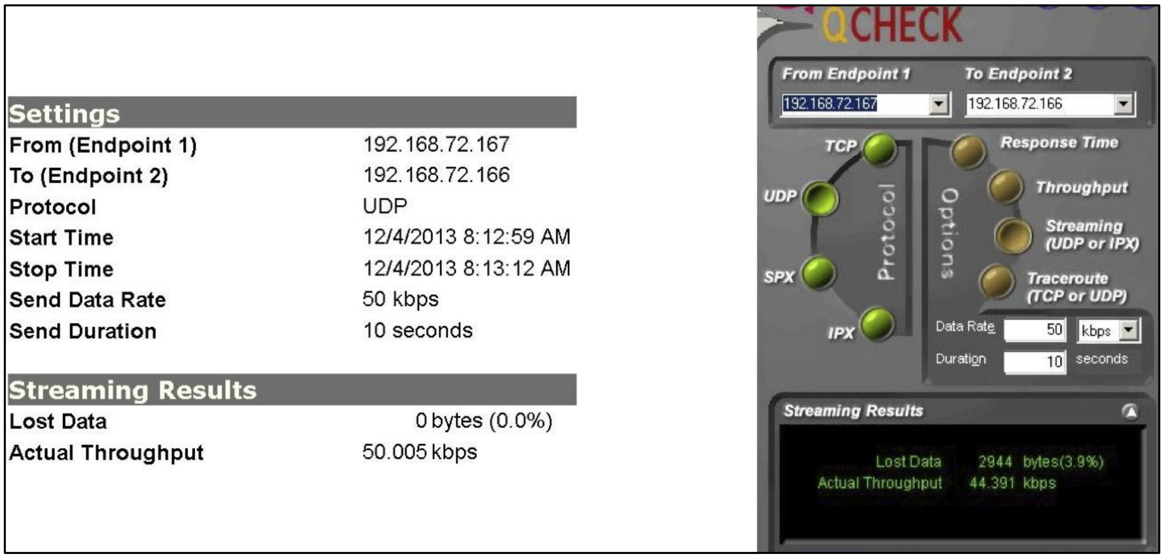

CF74-TB-04
Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller - Packet Scheduler Miniport
0
1K
10K
100K
1M
10M
6521 bps
Receive
0
1K
10K
100K
1M
10M
289 bps
Transmit
CF74-TB-04
Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller - Packet Scheduler Miniport
0
1K
10K
100K
1M
33.6 Kbps
Receive
0
1K
10K
100K
1M
20.0 Kbps
Transmit

Figure 12. SolarWinds Band Width Gauges

4. Packet Loss

To provide packet loss data to the network manager, the Qcheck UDP and SolarWinds Response Time applications were chosen. In figure 13, the Qcheck UDP baseline shows that 50 kbps could be transmitted with zero packet loss had under ideal settings. Once the network was deployed, the application measured 44kbps was transmitted with under 3 kbps or 3.9 percent packet loss. Figure 14 depicts a graph from the SolarWinds Response Time application. The baseline also shows no packet loss within the network while in the lab environment, but once the network was deployed and interference was introduced to the network, packet loss began to appear indicated by the red lines on the graph.



Settings

From (Endpoint 1)	192.168.72.167
To (Endpoint 2)	192.168.72.166
Protocol	UDP
Start Time	12/4/2013 8:12:59 AM
Stop Time	12/4/2013 8:13:12 AM
Send Data Rate	50 kbps
Send Duration	10 seconds

Streaming Results

Lost Data	0 bytes (0.0%)
Actual Throughput	50.005 kbps

From Endpoint 1: 192.168.72.167
To Endpoint 2: 192.168.72.166
Data Rate: 50 kbps
Duration: 10 seconds

Streaming Results
Lost Data 2944 bytes(3.9%)
Actual Throughput 44.391 kbps

Figure 13. Qcheck UDP Throughput

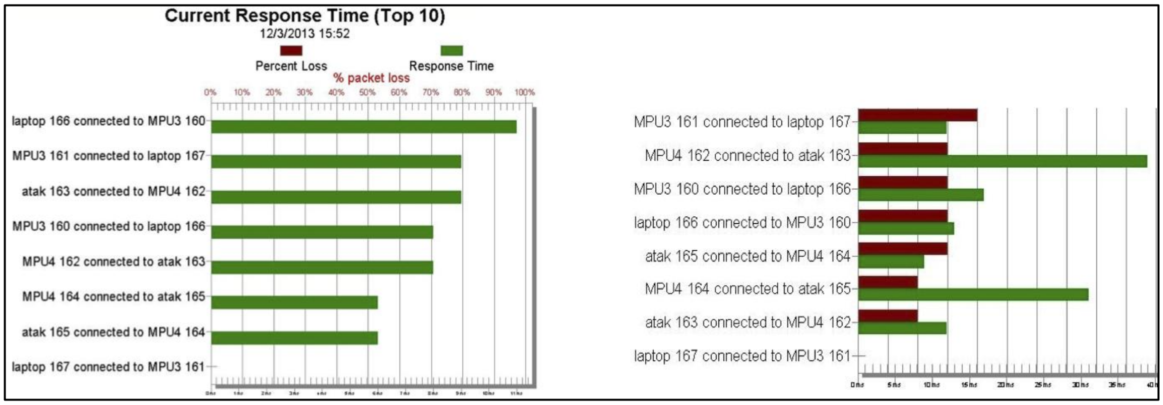


Figure 14. SolarWinds Response Time

5. Protocol Monitor

The SNMP Real Time Graph from SolarWinds was used to depict the different protocols in place for monitoring the network. Figure 15 shows a timeline of the established network. Each color indicates a protocol, and the amount of throughput each is sending throughout. The spikes in the graph indicate when the prospected protocol is in use, and the extent of the throughput.

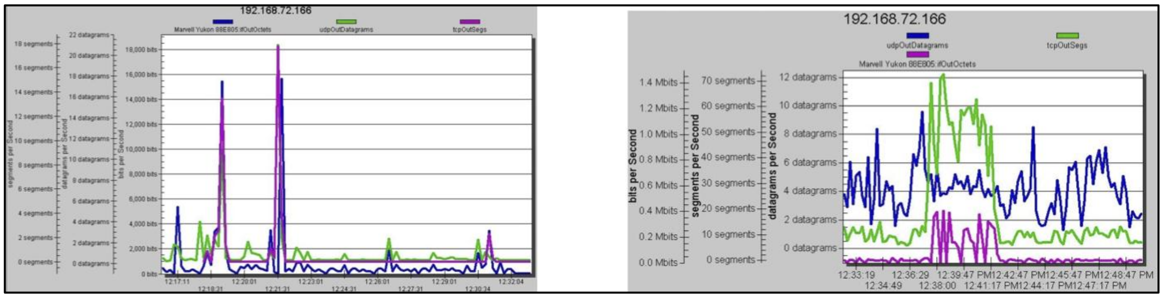


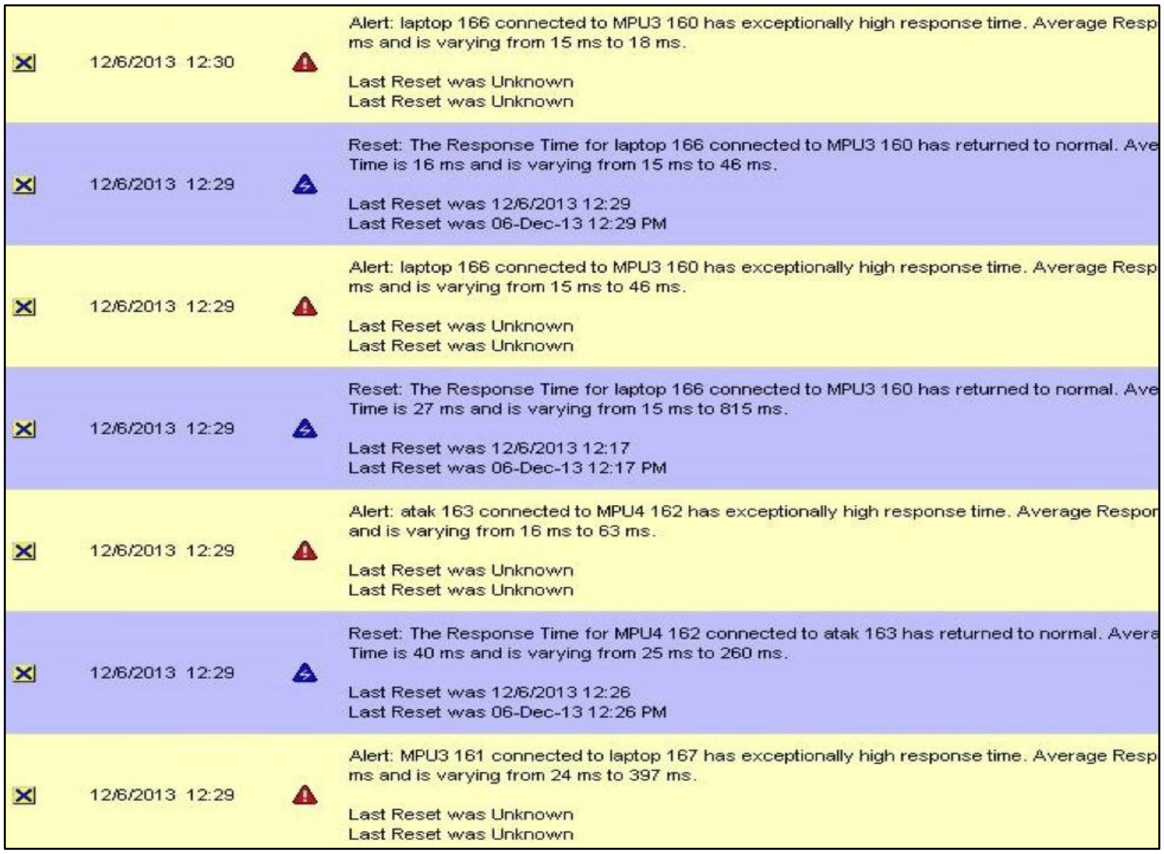
Figure 15. SolarWinds SNMP Real Time Graph

6. Voice/Data Exchange

To test the exchange of voice, the experiment team members periodically conducted simple radio checks using the WR devices to insure connectivity. Data was also transferred using the WR devices by sending pictures taken while roaming throughout the ship.

7. Alarms

The SolarWinds Network Performance Event Monitor was chosen to indicate changes within the network. This application is depicted in figure 16, and allowed the network manager the ability to see significant changes in node performances. An example of what the application provided was notifications alerting on high response times from specific nodes.



☒	12/6/2013 12:30	▲	Alert: laptop 166 connected to MPU3 160 has exceptionally high response time. Average Resp ms and is varying from 15 ms to 18 ms. Last Reset was Unknown Last Reset was Unknown
☒	12/6/2013 12:29	△	Reset: The Response Time for laptop 166 connected to MPU3 160 has returned to normal. Ave Time is 16 ms and is varying from 15 ms to 46 ms. Last Reset was 12/6/2013 12:29 Last Reset was 06-Dec-13 12:29 PM
☒	12/6/2013 12:29	▲	Alert: laptop 166 connected to MPU3 160 has exceptionally high response time. Average Resp ms and is varying from 15 ms to 46 ms. Last Reset was Unknown Last Reset was Unknown
☒	12/6/2013 12:29	△	Reset: The Response Time for laptop 166 connected to MPU3 160 has returned to normal. Ave Time is 27 ms and is varying from 15 ms to 815 ms. Last Reset was 12/6/2013 12:17 Last Reset was 06-Dec-13 12:17 PM
☒	12/6/2013 12:29	▲	Alert: atak 163 connected to MPU4 162 has exceptionally high response time. Average Respor and is varying from 16 ms to 63 ms. Last Reset was Unknown Last Reset was Unknown
☒	12/6/2013 12:29	△	Reset: The Response Time for MPU4 162 connected to atak 163 has returned to normal. Avera Time is 40 ms and is varying from 25 ms to 260 ms. Last Reset was 12/6/2013 12:26 Last Reset was 06-Dec-13 12:26 PM
☒	12/6/2013 12:29	▲	Alert: MPU3 161 connected to laptop 167 has exceptionally high response time. Average Resp ms and is varying from 24 ms to 397 ms. Last Reset was Unknown Last Reset was Unknown

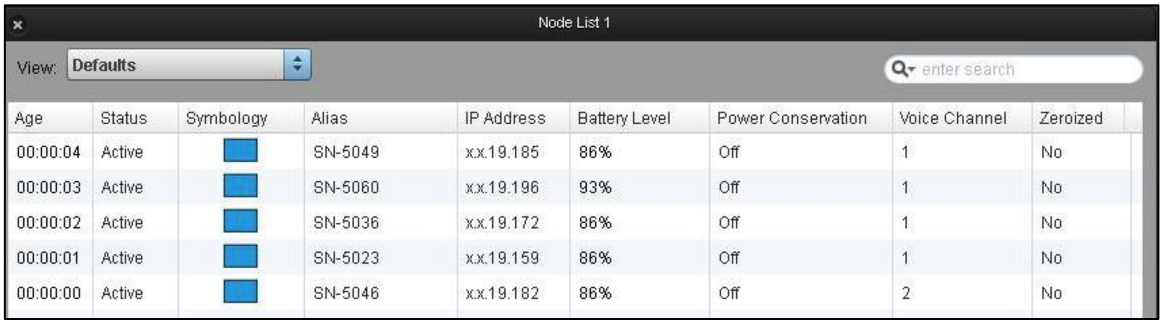
Figure 16. SolarWinds Network Performance Monitor Events

B. TRELLISWARE

This section will provide details of the data collected from the established WMN onboard the *ADM. Callaghan* using TW devices.

1. Node State

Figure 17 is the data capture display using the TW NMS as a baseline network within the lab environment. The TW NMS also provides information concerning the status of the devices' battery and current channel selection as well as the IP address for each node. Figure 18 is a data capture using the SolarWinds NMS as the network was deployed in testing onboard the ship environment. It provides the network manager additional information to include the response time and packet loss for each node.

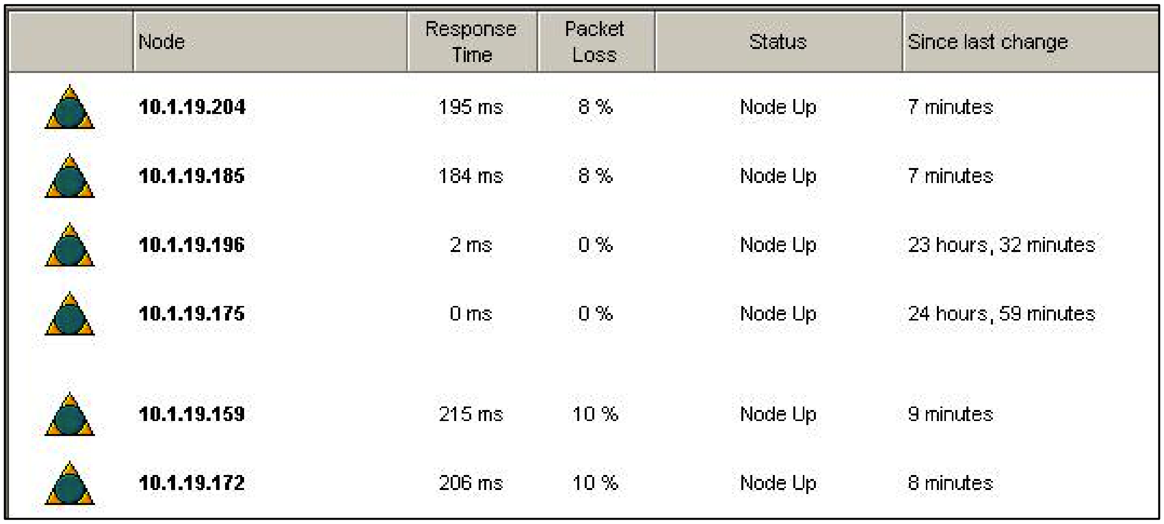


Node List 1

View: Defaults

Age	Status	Symbology	Alias	IP Address	Battery Level	Power Conservation	Voice Channel	Zeroized
00:00:04	Active	🟦	SN-5049	x.x.19.185	86%	Off	1	No
00:00:03	Active	🟦	SN-5060	x.x.19.196	93%	Off	1	No
00:00:02	Active	🟦	SN-5036	x.x.19.172	86%	Off	1	No
00:00:01	Active	🟦	SN-5023	x.x.19.159	86%	Off	1	No
00:00:00	Active	🟦	SN-5046	x.x.19.182	86%	Off	2	No

Figure 17. Trellisware Node List

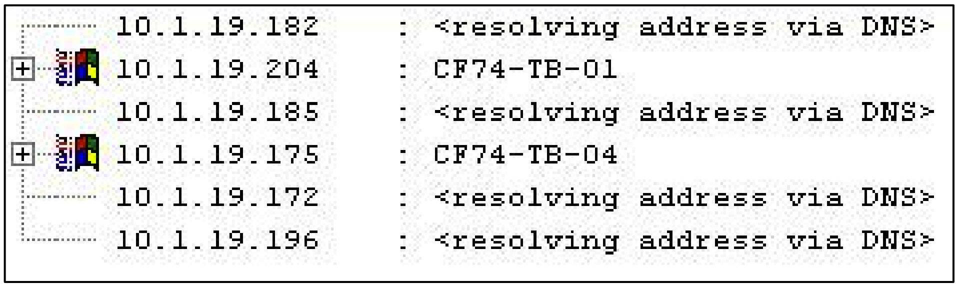


	Node	Response Time	Packet Loss	Status	Since last change
▲	**10.1.19.204**	195 ms	8 %	Node Up	7 minutes
▲	**10.1.19.185**	184 ms	8 %	Node Up	7 minutes
▲	**10.1.19.196**	2 ms	0 %	Node Up	23 hours, 32 minutes
▲	**10.1.19.175**	0 ms	0 %	Node Up	24 hours, 59 minutes
▲	**10.1.19.159**	215 ms	10 %	Node Up	9 minutes
▲	**10.1.19.172**	206 ms	10 %	Node Up	8 minutes

Figure 18. SolarWinds Network Monitor

2. Link State

Figure 19 is the NMS data capture using the SolarWinds IP Net Browser application. This was an attempt to map the network's links of both the baseline and execution. The TW devices are layer 2 devices; therefore, the NMS was unable to diagram the network topology other than the two endpoints of the network.

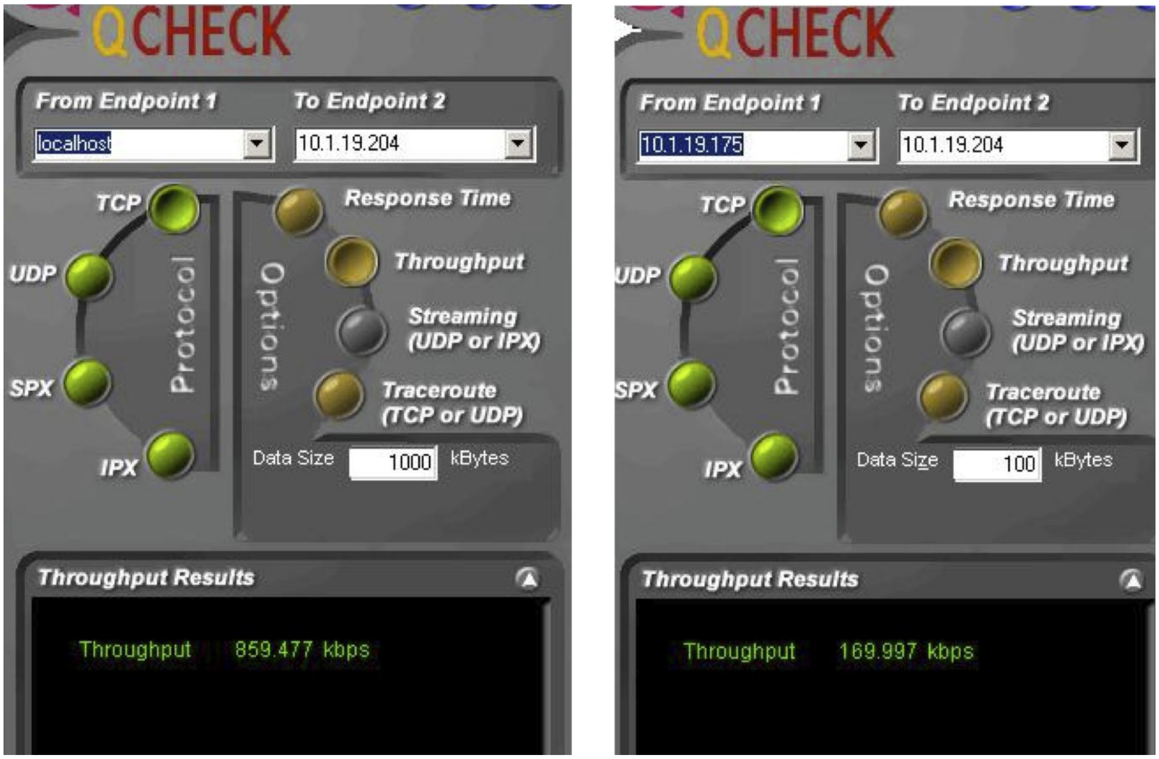


```
10.1.19.182     : <resolving address via DNS>
10.1.19.204     : CF74-TB-01
10.1.19.185     : <resolving address via DNS>
10.1.19.175     : CF74-TB-04
10.1.19.172     : <resolving address via DNS>
10.1.19.196     : <resolving address via DNS>
```

Figure 19. SolarWinds IP Network Browser

3. Throughput

Figures 20 and 21 depict the throughput measurements. Both Qcheck and SolarWinds NMS were used to determine the amount of data that the network was moving from endpoint to endpoint. The baseline for each NMS indicates the throughput each network can obtain under ideal environments while the other shows the actual throughput when deployed.



From Endpoint 1: localhost
To Endpoint 2: 10.1.19.204
Data Size: 1000 kBytes
Throughput Results
Throughput 859.477 kbps

From Endpoint 1: 10.1.19.175
To Endpoint 2: 10.1.19.204
Data Size: 100 kBytes
Throughput Results
Throughput 169.997 kbps

Figure 20. Qcheck TCP Throughput

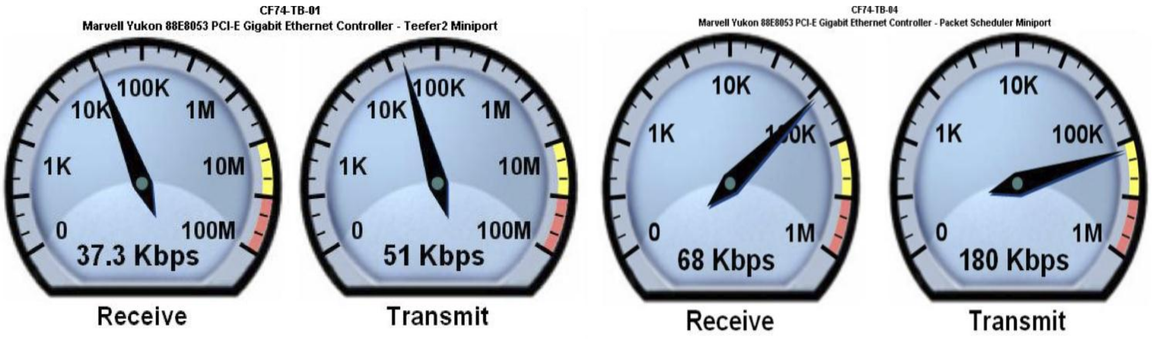

CF74-TB-01
Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller - Teefer2 Miniport
0
1K
10K
100K
1M
10M
100M
37.3 Kbps
Receive
0
1K
10K
100K
1M
10M
100M
51 Kbps
Transmit
CF74-TB-04
Marvell Yukon 88E8053 PCI-E Gigabit Ethernet Controller - Packet Scheduler Miniport
0
1K
10K
100K
1M
68 Kbps
Receive
0
1K
10K
100K
1M
180 Kbps
Transmit

Figure 21. SolarWinds Band Width Gauge

4. Packet Loss

To provide packet loss data to the network manager, the SolarWinds Response Time application was chosen. In figure 22, two graphs from the SolarWinds Response Time application is shown. The baseline also shows minor packet loss within the network while in the lab environment, but once the network was deployed and interference was introduced to the network, packet loss began to appear indicated by the red lines on the graph.

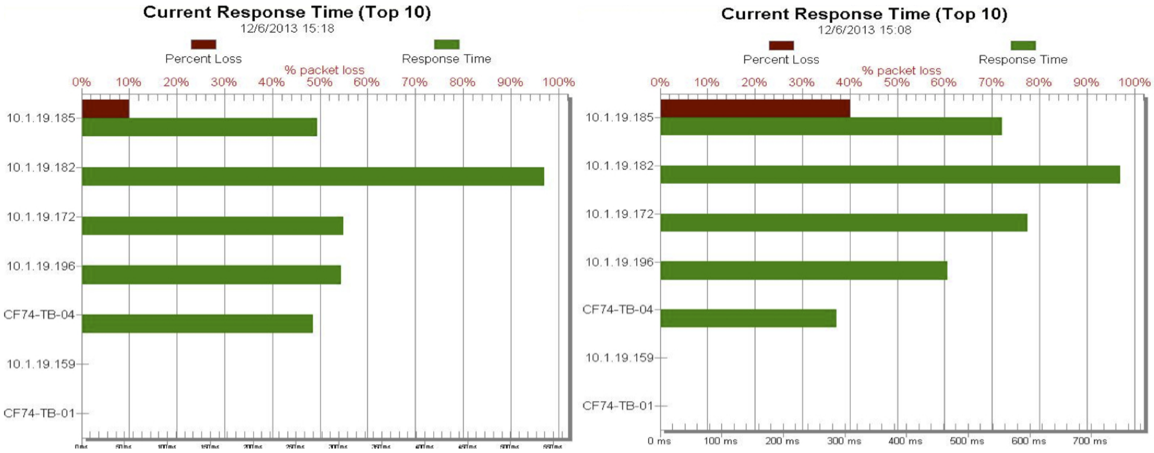


Figure 22. SolarWinds Current Response Time

5. Protocol Monitor

The SNMP Real Time Graph from SolarWinds was used to depict the different protocols in place for monitoring the network. Figure 23 shows a timeline of the established network. Each color indicates a protocol, and the amount of throughput each is sending throughout. The spikes in the graph indicate when the prospected protocol is in use, and the extent of the throughput.

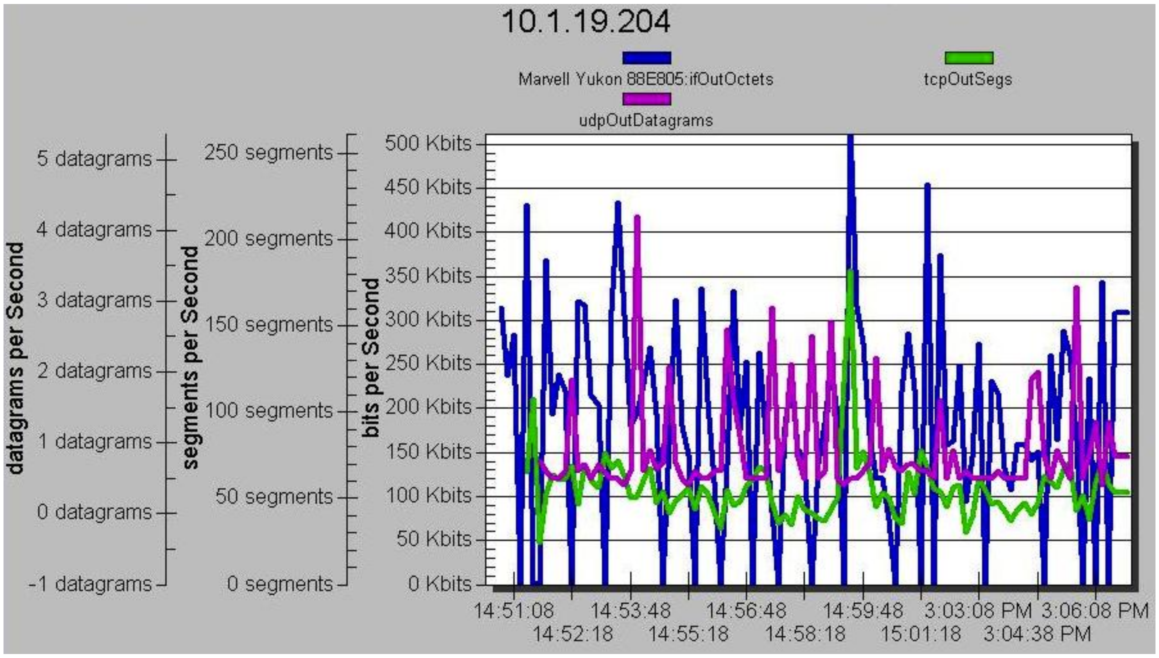


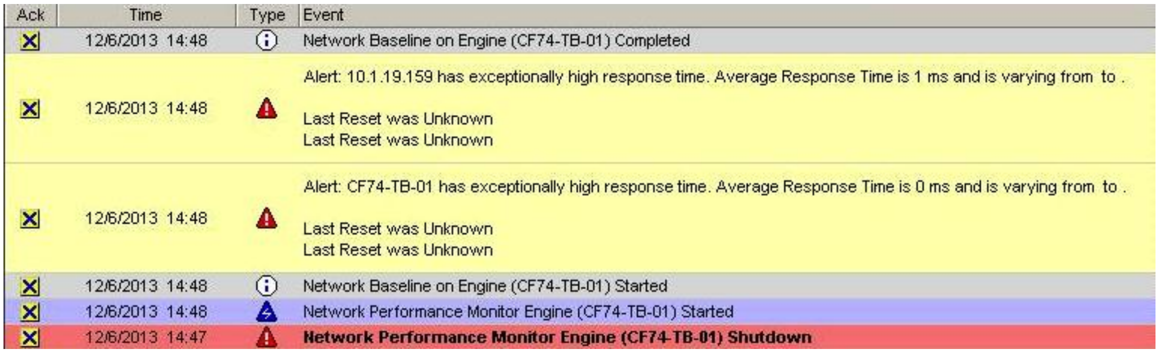
Figure 23. SolarWinds SNMP Real-Time Graph

6. Voice/Data Exchange

To test the exchange of voice, the experiment team members periodically conducted simple radio checks using the TWdevices to insure connectivity. Data was also transferred using the devices by transferring a constant stream of files from endpoint to endpoint through a generic chat application, but is not depicted. The file transfer was intended to further stress the communication capabilities of the devices as the team members roamed throughout the ship.

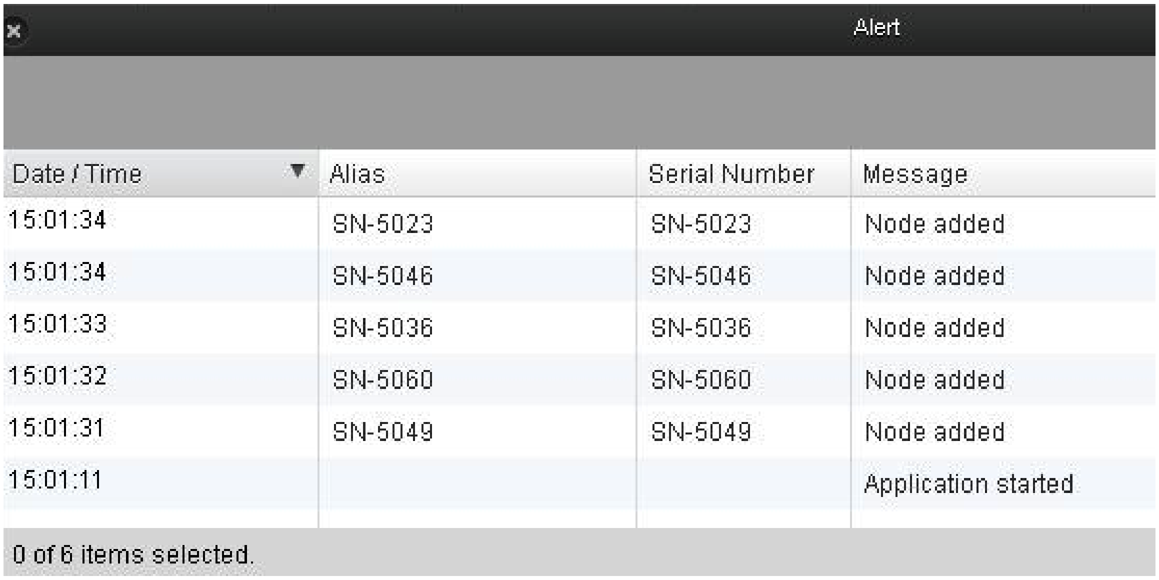
7. Alarms

The SolarWinds Network Performance Event Monitor was chosen to indicate changes within the network. This application is depicted in figure 24, and allowed the network manager the ability to see significant changes in node performances. An example of what the application provided was notifications alerting on high response times from specific nodes. Figure 25 is an alert application provided by the TW NMS. It displays information to the network manager about any changes in a node's status and a corresponding time stamp.



Ack	Time	Type	Event
☒	12/6/2013 14:48	ⓘ	Network Baseline on Engine (CF74-TB-01) Completed
☒	12/6/2013 14:48	⚠	Alert: 10.1.19.159 has exceptionally high response time. Average Response Time is 1 ms and is varying from to . Last Reset was Unknown Last Reset was Unknown
☒	12/6/2013 14:48	⚠	Alert: CF74-TB-01 has exceptionally high response time. Average Response Time is 0 ms and is varying from to . Last Reset was Unknown Last Reset was Unknown
☒	12/6/2013 14:48	ⓘ	Network Baseline on Engine (CF74-TB-01) Started
☒	12/6/2013 14:48	⚠	Network Performance Monitor Engine (CF74-TB-01) Started
☒	12/6/2013 14:47	⚠	**Network Performance Monitor Engine (CF74-TB-01) Shutdown**

Figure 24. SolarWinds Network Performance Monitor



Alert

Date / Time ▼	Alias	Serial Number	Message
15:01:34	SN-5023	SN-5023	Node added
15:01:34	SN-5046	SN-5046	Node added
15:01:33	SN-5036	SN-5036	Node added
15:01:32	SN-5060	SN-5060	Node added
15:01:31	SN-5049	SN-5049	Node added
15:01:11			Application started

0 of 6 items selected.

Figure 25. Trellisware Alerts

C. ANALYSIS

For the purpose of testing WMN applications for USCG VBSS boarding operations, this section will describe the strengths and weaknesses of using the WR and TW communication devices to achieve the USCG communication parameters.

1. WaveRelay

The WR network used a network manager onboard the SFPD patrol craft to capture data throughout the experiment. Based on the USCG communication criteria, the WR devices were effective in establishing a WMN between the SFPD patrol craft and the communications liaison positioned topside onboard the SS O'Brien. In the initial phase of the experiment, the WR devices were configured in accordance with Appendix A. to establish that the system remained an effective means to transmit voice and data among all network devices. The team members tested each device individually to show that voice and data was able to pass throughout the network. The ability for the network manager to track individual nodes was provided by the NMSs in basic forms of an up or down status, and packet loss. The NMS functions were also established as well to insure that the manager could see each network node, and that the proper data could be captured. The NMSs could capture throughput information passed between the communications liaison and SFPD patrol craft, but not between individual nodes.

After a successfully established network, the next phase of the experiment began, which was to expand the distance between nodes, and simultaneously expanding the mesh topology. The WR devices were sent into the interior of the *SS O'Brien*. The ability to maintain communications from the nodes became immediately difficult due to the inability to overcome the environment's interferences. Nodes in close proximity were able to communicate using voice, but were isolated from the network manager. Therefore, the network was unable to sufficiently expand to a distance useful to a VBSS team. If a node dropped a connection from the network, the network manager was immediately notified by the NMS alert applications, and the communication liaison was notified. The NMS was found to be useful in basic situational awareness applications, but was unable to assist in troubleshooting. The NMSs were cumbersome to navigate in such a dynamic operation, and data was difficult to capture effectively. The WR devices were found to work well as last mile connection for networks, but were unable to accomplish the required USCG communication parameters once deployed within the skin of the ship.

2. Trellisware

The TW WMN used two endpoints for the network to test the USCG communication parameters. Different from the initial SS O'Brien setup, the network began in an extended topology rather than expanding from a central location. The network manager used the first endpoint located on the weather decks midships. The second endpoint was located below decks approximately four levels. This distance was used without relay nodes to show that the endpoints could not maintain satisfactory voice communications. Once the second endpoint was in place, the relay nodes were initiated. The next phase of the test established that each node could establish voice communications effectively, and that each team member could communicate using voice. The network manager was able to monitor the nodes at this point using the NMS applications in basic forms of up or down status, packet loss, and battery levels. To test data capabilities, throughput data was measured between endpoints using NMSs, but not between individual nodes. For the purpose of passing data, the endpoints employed a generic chat room application. Because this network did not contain devices able to take pictures, the below deck endpoint transferred a set of files sufficient enough to maintain a continuous flow of data, and to place additional strain on the network communication links. This allowed the network manager to effectively capture the required data to prove that it was possible with TW devices.

The next phase of the tests were to have the remaining nodes increase the distance between communication links. The devices were effective in maintaining voice communications throughout the remainder ship's environment. To further test the boundaries of the communication limits, a node was sent outside of the ship to the pier. The node was approximately 1,000 feet from the ship before communication disruptions began to appear. The NMSs allowed the network manager to monitor the status of each node effectively throughout the tests. The NMSs were still found to be cumbersome in their deployment because the network manager had to switch between applications to effectively monitor additional aspects of the network. Although the nodes never lost a voice communication link, the data transfer test revealed that passing data was much slower than what was expected.

V. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSION

The results of this study offers the examination of an ad hoc WMN that can be established to conduct VBSS operations on large freighter vessels using commercially available technology without depending on existing communication infrastructures. The tests further proved that existing technologies are available to conduct effective operations in a MIO environment. These technologies must now be translated into useful operationally ready tools to increase future VBSS missions.

B. RECOMMENDATIONS FOR FUTURE RESEARCH

1. Increase Network Management System Capabilities

The proprietary software provided by the WR and TW devices were found to be an ineffective means to fully capture the required information a network manager needs. Additional monitoring software was needed to cover the information gaps, and created a variety of applications that had to be navigated by the network manager. Future NMSs should provide the network manager with a more user friendly means to navigate required applications, and manage different forms of communication. It is recommended that future networks test the Mobile Field Kit application software for a viable means of network management.

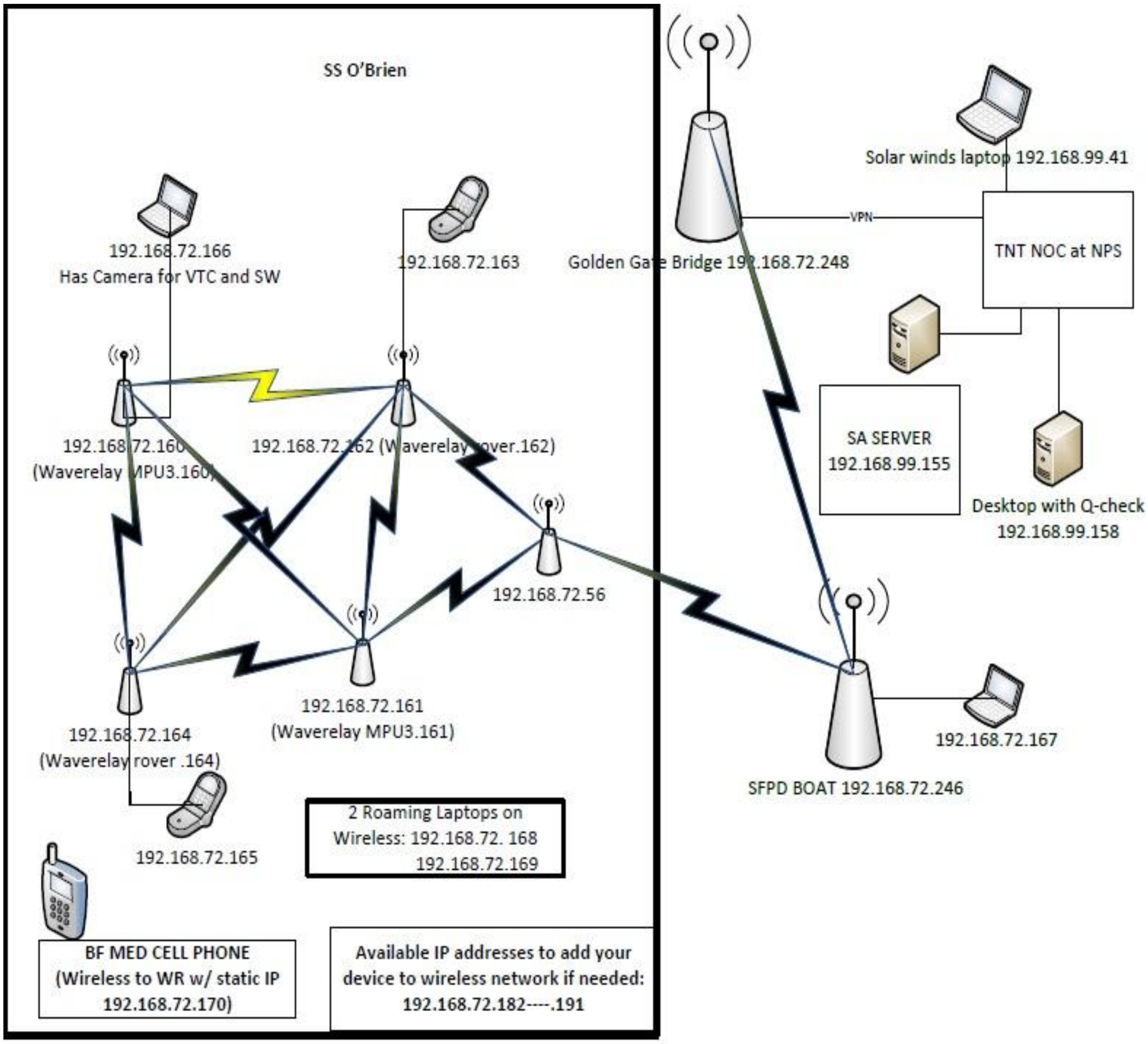
2. Additional Collaborative Tools

To further expand the capabilities of WMNs, additional equipment should be added to communication devices. The equipment should be interchangeable among devices, and provide an effective means for boarding teams to capture and transmit video, picture stills, and biometric feedback. This would increase the boarding teams efficiency and effectiveness. Much like the WR devices, the TW devices need the ability to attach to mobile data capturing devices such as sensors or smartphones. This will also allow devices like TW to expand the mesh network from a central location rather than starting from a topology with already divided endpoints.

3. Expand the Mesh

The future testing of SDRs in a WMN should increase the distance between nodes onboard large freighter vessels to fully test the boundaries of voice and data communications. In addition, the connection to a support vessel should be incorporated when possible. This will test the ability to bridge the gap between the boarding team and the shadowing support vessel, which increases the safety of operations and situational awareness for operation commanders.

APPENDIX A. SS O’BRIEN WMN TOPOLOGY



<u>SF Experiment → Items of Interest</u>

- **Experiment on SS O’Brien**
    - qCheck
        - TCP response time & throughput
        - UDP response time, throughput, and streaming
    - SolarWinds
        - Bandwidth Gauge
        - Errors Today
        - In-Out BPS
        - IP Net Discovery
        - MAC Address Discovery
        - Network Monitor Events
        - Network Monitor

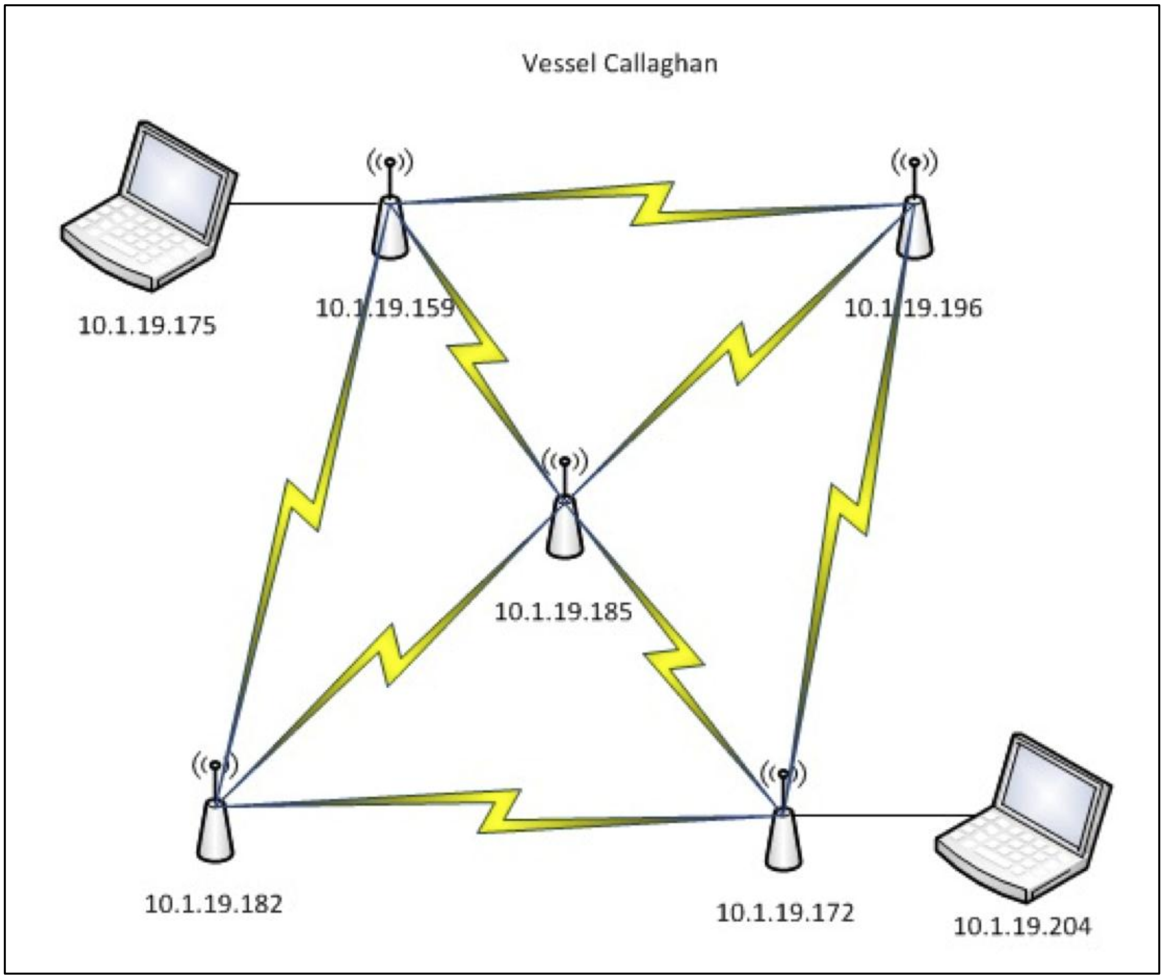
- Ping Sweep
- Response Time
- SNMP Sweep

- SNMP Real Time GraphsWaveRelay
    - Channel Plan
    - IP Flow List
    - Neighbor SNR
    - Network Info
    - Network Traffic Load
    - TCP Throughput

Gear List

- Pen and paper x 2
- WaveRelay
    - MPU3 x 2 + two power adapters
    - MPU4 x 2
    - Quad Radio Router setup
- ATAK x 2 + charging cord x 1 (Brandon has these)
- Laptop x 4 + power cord x 2
- Accessories
    - Charger base
    - Radio batteries x 8
    - Extension cord x 2
    - Headset x 4
    - Cat 5 x 3
    - Cat 5 crossover x 1
    - AA batteries x 48
    - Power strip
    - Cameras for laptops x 2
    - UPS

APPENDIX B ADM. CALLAGHAN WMN TOPOLOGY



THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Akyildiz, I. & Wang, X. (2005). A survey on wireless mesh networks. *IEEE Communications Magazine*, 43, 445–487. DOI: 10.1109/MCOM.2005.1509968

Alvestrand, H. (2004). *Internet engineering task force best current practice*. Retrieved from https://www.ietf.org/rfc/rfc3935.txt

Barker, E. (2009, April 4). *VBSS: Evolving with the mission*. Retrieved from http://www.navy.mil/submit/display.asp?story_id=44692

Bartlett, D., Donaldson, I., & Stewart, V. (2013). USCG long haul wireless network: boarding team to cutter. Unpublished manuscript, Naval Postgraduate School, Monterey, CA.

Bieszad, A., Pagurek, B., & White, T. (2009). Mobile Agents for Network Management. *IEEE Communications Surveys and Tutorials, 1,* 2–9. DOI: 10.1109/COMST.1998.5340400

Bruno, R., Conti, M., & Gregori, E. (2005). Mesh networks: commodity multihop ad hoc networks. *IEEE Communications Magazine*, *43*, 123–131. DOI: 10.1109/MCOM.2005.1404606

Centers for Disease Control and Prevention (n.d.). Shannon's capacity equation. Retrieved from http://www.cdc.gov/niosh/mining/content/emergencymanagementandresponse/commtracking/advcommtrackingtutorial2.html

Dean, T. (2013). *Network + guide to networks*. 6th ed. Boston: Course Technology.

Djohara B., Hafid, A., & Gendreau, M. (2012). Wireless Mesh Networks Design—A Survey. *IEEE Communications Surveys &Tutorials*, *14*, 299–310. DOI: 10.1109/SURV.2011.042711.00007

Edelkind, E. (2012). Enhanced VBSS. *Marine Corps Gazette, 96*(8), 36–38. Retrieved from http://search.proquest.com/docview/1032950116?accountid=12702

Institute of Electrical and Electronics Engineers, IEEE 802. (2012). *SNMP MIBS*. Retrieved from http://www.ieee802.org/1/pages/MIBS.html

Jun, J., & Sichitiu, M. (2003). The nominal capacity of wireless mesh networks. *IEEE Wireless Communications,* 10, 8–14. DOI: 10.1109/MWC.2003.1241089

Mesh Networks. (2013). *Mesh networks: Why mesh*. Retrieved from http://www.meshnetworks.com/why-mesh/

Mesh Networks. (2013). *Mesh networks: Technology overview*. Retrieved from http://www.meshnetworks.com/

Mitola, J. (1999). Software radio architecture: A mathematical perspective. *IEEE Journal on Selected Areas in Communications*, 17, 514–538. DOI: 10.1109/49.761033

Motorola. (2006). *Mesh networks: Delivering IP-based seamless mobility in municipal and ad hoc wireless networks* (white paper). Retrieved from http://www.motorola.com/innovators/pdfs/Mesh-Ntwks-WP-7.24.06.pdf

Motorola. (2005). *Mesh networks: Decentralized, self-forming, self-healing networks that achieve unprecedented coverage, throughput, flexibility, and cost efficiency* (position paper). Retrieved from http://www.motorolasolutions.com/web/Business/Products/Wireless%20Broadband%20Networks/Mesh%20Networks/_Documents/_static%20file/wp_technology_position_paper.pdf?localeId=111

The National Liberty Ship Memorial. (n.d.). SS Jeremiah O'Brien. Retrieved from http://www.ssjeremiahobrien.org/

NavSource Online. (n.d.). GTS Admiral W. M. Callaghan (AKR-1001). Retrieved from http://www.navsource.org/archives/09/54/541001.htm

Nguyen, H., & Baker, M. (2012). Characteristics of a maritime interdiction operations unmanned ground vehicle. *Proceedings of the International Society for Optics and Photonics (SPIE).* San Diego, CA, 8387 83871G. DOI: 101117/12.918089

Persistent Systems. (n.d.). Man portable unit 3. Retrieved from http://www.persistentsystems.com/products_2a.php see notes sheet for how to cite if both author and year are the same.

Persistent Systems. (n.d.). Man portable unit 4. Retrieved from http://www.persistentsystems.com/products_7a.php

Persistent Systems. (2012). *Technology*. Retrieved from http://www.persistentsystems.com/pdf/WaveRelay_WhitePaper_Technology_01.pdf

Persistent Systems. (2012). *Department of Defense*. Retrieved from http://www.persistentsystems.com/pdf/WaveRelay_WhitePaper_DepartmentOfDefense_01.pdf

Rank, E. (2012, March). *Manpower issues involving visit, board, search, and seizure (VBSS)* (Master's thesis). Retrieved from http://www.acquisitionresearch.net

Schechter, E. (2013). Mobile ad hoc networks end reliance on infrastructure. Retrieved from http://www.c4isrnet.com/article/M5/20131113/C4ISRNET04/311130028/Mobile-ad-hoc-networks-end-reliance-infrastructure?odyssey=nav%7Chead

Stavroulakis, G. (2006). *Rapidly deployable, self-forming, wireless networks for maritime interdiction operations* (Master's thesis). Retrieved from http://www.acquisitionresearch.net

Subramanian, M. (2011). *Network management: Principles and practice*. India: Dorling Kindersley.

Sundall, J., Carroll, C. (2008, June). *Transforming data and metadata into actionable intelligence and information within the maritime domain* (Master's thesis). Retrieved from http://www.acquisitionresearch.net

Tabassam, A. A., Kalsait, S., & Suleman, M. U. (2011, March). Building software-defined radios in MATLAB Simulink: A step towards cognitive radios. *Computer MOdleing and Simulation (UKSim), 13th International Conference on Computer Modeling and Simulation*. DOI 10.1109/UKSIM.2011.100.

Trellisware Technologies, Products. (2014). Scalable tactical MANET communications. Retrieved from http://www.trellisware.com/products/manet-products/cheetahnet-tw-220/

Vann, C. A. (2012), *Implementation of software programmable radios to form ad-hoc meshed networks to enhance maritime interception operations* (Master's thesis). Retrieved from http://www.acquisitionresearch.net

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California